

# **MATRIX E5 Series Modules (5H1xx and 5G1xx)**

## **Local Management User's Guide**



## NOTICE

Enterasys Networks and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS AND ITS LICENSORS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS AND ITS LICENSORS HAVE BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.  
35 Industrial Way  
Rochester, NH 03866-5005

Enterasys Networks, Inc. is a subsidiary of Cabletron Systems, Inc.

© 2001 by Enterasys Networks, Inc.  
All Rights Reserved  
Printed in the United States of America

Order Number: 9033583-01 March 2001

LANVIEW is a registered trademark of Enterasys Networks or its licensors; SmartSwitch and Enterasys Networks are trademarks of Enterasys Networks or its licensors. SPECTRUM is a registered trademark of Aprisma Management Technologies or its licensors.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

---

# ENTERASYS NETWORKS, INC. PROGRAM LICENSE AGREEMENT

## BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement (“Agreement”) between You, the end user, and Enterasys Networks, Inc. (“Enterasys”) that sets forth your rights and obligations with respect to the Enterasys software program (“Program”) in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS (603) 332-9400. Attn: Legal Department.

**1. LICENSE.** You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Enterasys.

**2. OTHER RESTRICTIONS.** You may not reverse engineer, decompile, or disassemble the Program.

**3. APPLICABLE LAW.** This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

**4. EXPORT REQUIREMENTS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People’s Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

---

**5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Product (i) was developed solely at private expense; (ii) contains “restricted computer software” submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

**6. EXCLUSION OF WARRANTY.** Except as may be specifically provided by Enterasys in writing, Enterasys makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

ENTERASYS DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY ENTERASYS IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

**7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS ENTERASYS PRODUCT, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.



---

# Contents

Figures .....	ix
Tables.....	xi

## ABOUT THIS GUIDE

Using This guide .....	xiii
Structure of This Guide .....	xiii
Related Documents.....	xv
Document Conventions.....	xv
Typographical and Keystroke Conventions.....	xvi
Getting Help .....	xvii

## 1 INTRODUCTION

1.1 Overview .....	1-1
1.1.1 The Management Agent .....	1-2
1.1.2 In-Band vs. Out-of-Band .....	1-2
1.2 Navigating Local Management Screens .....	1-3
1.3 Local Management Requirements .....	1-3

## 2 LOCAL MANAGEMENT REQUIREMENTS

2.1 Management Terminal Setup.....	2-1
2.1.1 Console Cable Connection .....	2-1
2.1.2 Management Terminal Setup Parameters .....	2-2
2.2 Telnet Connections .....	2-4

## 3 ACCESSING LOCAL MANAGEMENT

3.1 Navigating Local Management Screens .....	3-1
3.2 Accessing Local Management Screens.....	3-3
3.3 Password Screen .....	3-4
3.4 Factory Defaults .....	3-5

## 4 MAIN MENU SCREENS

4.1 Main Menu .....	4-2
---------------------	-----

---

<b>5</b>	<b>SYSTEM INFORMATION MENU SCREENS</b>	
5.1	System Information Menu Screen.....	5-1
5.1.1	Displaying System Information .....	5-2
5.1.2	Displaying Switch Version and Module Information.....	5-4
<b>6</b>	<b>MANAGEMENT SETUP MENU SCREENS</b>	
6.1	Management Setup Menu Screen .....	6-2
6.2	Changing the Network Configuration .....	6-3
6.2.1	IP Configuration .....	6-4
6.2.2	IP Connectivity Test (Ping) .....	6-6
6.2.3	HTTP Configuration .....	6-7
6.3	Configuring the Serial Port.....	6-8
6.4	Assigning SNMP Parameters.....	6-10
6.4.1	Configuring Community Names.....	6-12
6.4.2	Configuring IP Trap Managers.....	6-13
6.5	Console Login Configuration.....	6-14
6.6	Setting the Startup Configuration.....	6-15
6.7	Downloading System Software .....	6-16
<b>7</b>	<b>DEVICE CONTROL MENU SCREENS</b>	
7.1	Configuring the Switch .....	7-1
7.2	Configuring Port Parameters.....	7-4
7.3	Viewing the Current Port Configuration.....	7-6
7.4	Using the Spanning Tree Algorithm .....	7-8
7.4.1	Configuring STA Bridge .....	7-9
7.4.2	Configuring STA for Ports.....	7-11
7.5	Viewing the Current Spanning Tree Configuration.....	7-13
7.5.1	Displaying the Current STA Bridge.....	7-14
7.5.2	Displaying the Current STA for Ports or Modules .....	7-16
7.6	Using a Mirror Port for Analysis .....	7-18
7.7	Configuring SmartTrunks .....	7-19
7.7.1	IGMP Multicast Filtering.....	7-21
7.8	Configuring IGMP.....	7-22
7.9	Configuring Bridge MIB Extensions .....	7-23
7.10	Configuring Traffic Classes.....	7-25
7.10.1	Port Priority Configuration.....	7-25
7.10.2	802.1P Port Traffic Class Information .....	7-26
7.11	Configuring Virtual LANs.....	7-27
7.12	802.1Q VLAN Base Information.....	7-28
7.13	802.1Q VLAN Current Table Information.....	7-29
7.14	802.1Q VLAN Static Table Configuration.....	7-30



7.15	802.1Q VLAN Port Configuration .....	7-32
7.16	Configuring Static Unicast Addresses .....	7-34

## **8 NETWORK MONITORING MENU SCREENS**

8.1	Monitoring the Switch .....	8-1
8.2	Displaying Port Statistics .....	8-2
8.3	Displaying RMON Statistics .....	8-4
8.4	Displaying the Unicast Address Table .....	8-6
8.5	Displaying the IP Multicast Registration Table .....	8-8

## **9 SYSTEM RESTART MENU SCREEN**

9.1	Resetting the System .....	9-1
9.2	Logging Off the system .....	9-2

## **10 CONFIGURING AND MONITORING THE SWITCH**

10.1	Common Tasks .....	10-1
10.2	Setting Password Protection .....	10-2
10.3	Assigning an IP Address .....	10-3
10.4	Checking Network Configuration Status .....	10-3
10.5	Connecting via Telnet .....	10-3
10.6	Setting SNMP Management Access .....	10-3
10.7	Viewing Switch Statistics .....	10-4
10.8	Configuring Port Mirroring .....	10-4
10.9	Downloading a Software Upgrade .....	10-5
	10.9.1 Downloading via the Serial Port .....	10-5
	10.9.2 Downloading via TFTP .....	10-6
10.10	Configuring Spanning Tree Parameters .....	10-7
10.11	Configuring VLANs .....	10-7
10.12	Configuring Class of Service .....	10-8
10.13	Configuring IGMP .....	10-8
10.14	Configuring Port Operation .....	10-9
10.15	Configuring the Unicast Address Table .....	10-10
	10.15.1 Port Locking .....	10-11
	10.15.2 Unlocking the Port .....	10-11
10.16	Setting a Default Gateway .....	10-12
10.17	Configuring SmartTrunks .....	10-12

## **11 SNMP MANAGEMENT**

11.1	The SNMP Protocol .....	11-1
11.2	MIB Objects .....	11-2

---

11.2.1	RFC 1213 (MIB II).....	11-2
11.2.2	RFC 1493 (BRIDGE MIB).....	11-3
11.2.3	RFC 1573 (INTERFACES EVOLUTION MIB).....	11-3
11.2.4	RFC 1643 (ETHERNET-LIKE MIB).....	11-3
11.2.5	RFC 1757 (RMON MIB).....	11-3
11.2.6	IEEE 802.1Q (Q MIB).....	11-4
11.3	Enterasys Proprietary MIB Extensions.....	11-4
11.4	Compiling MIB Extensions: Enterasys Website.....	11-4

## **A SPANNING TREE CONCEPTS**

A.1	General.....	A-1
A.1.1	Spanning Tree Features.....	A-1
A.2	Spanning Tree Protocol in a Network.....	A-2
A.3	Spanning Tree Protocol Parameters.....	A-3
A.3.1	Spanning Tree Protocol Operation.....	A-4
A.3.2	Communicating Between Bridges.....	A-4
A.3.3	Selecting a Root Bridge and Designated Bridges.....	A-4
A.3.4	Selecting Designated Ports.....	A-4
A.3.5	Handling Duplicate Paths.....	A-5
A.3.6	Remapping Network Topology.....	A-5

## **B VIRTUAL LANs (VLANs)**

B.1	VLANs and Frame Tagging.....	B-1
B.2	VLAN Configuration.....	B-2
2.3	Forwarding Tagged/Untagged Frames.....	B-3
B.4	Forwarding Traffic with Unknown VLAN Tags.....	B-3

## **C CLASS OF SERVICE**

## **D IP MULTICAST FILTERING**

## **INDEX**

---

# Figures

Figure		Page
2-1	Management Terminal Connection .....	2-2
3-1	Local Management Screen Hierarchy .....	3-2
3-2	Sample Main Menu .....	3-3
3-3	Password Screen .....	3-4
4-1	Main Menu.....	4-2
5-1	System Information Menu Screen .....	5-1
5-2	System Information Screen .....	5-2
5-3	Switch Information Screen .....	5-4
6-1	Management Setup Menu Screen.....	6-2
6-2	Network Configuration Menu Screen .....	6-3
6-3	IP Configuration Screen .....	6-4
6-4	IP Connectivity Test Screen .....	6-6
6-5	HTTP Configuration Screen .....	6-7
6-6	Serial Port Configuration Screen.....	6-8
6-7	SNMP Configuration Menu Screen .....	6-10
6-8	SNMP Communities Screen.....	6-12
6-9	IP Trap Managers Screen .....	6-13
6-10	Console Login Configuration Screen.....	6-14
6-11	Startup Configuration Screen .....	6-15
6-12	TFTP Download Screen .....	6-17
7-1	Device Control Menu Screen .....	7-2
7-2	Port Configuration Screen .....	7-4
7-3	Port Information Screen .....	7-6
7-4	Spanning Tree Configuration:Selection Menu Screen .....	7-8
7-5	STA Bridge Configuration Screen .....	7-9
7-6	STA Tree Port Configuration Screen.....	7-11
7-7	Spanning Tree Information: Selection Menu Screen.....	7-13
7-8	STA Bridge Information Screen.....	7-14
7-9	STA Port Information Screen .....	7-16
7-10	Mirror Port Configuration Screen.....	7-18
7-11	SmartTrunking Configuration Screen .....	7-20
7-12	IGMP Configuration Screen .....	7-22
7-13	Extended Bridge Configuration Screen .....	7-23
7-14	802.1P Configuration Menu Screen .....	7-25
7-15	802.1P Port Priority Configuration Screen .....	7-26

---

Figure		Page
7-16	802.1P Port Traffic Class Information Screen .....	7-27
7-17	802.1Q VLAN Base Information Screen .....	7-28
7-18	802.1Q VLAN Current Table Information Screen .....	7-29
7-19	802.1Q VLAN Static Table Configuration Screen .....	7-31
7-20	802.1Q VLAN Port Configuration Screen .....	7-32
7-21	Static Unicast Address Table Configuration Screen .....	7-34
8-1	Network Monitor Menu Screen .....	8-1
8-2	Port Statistics Screen .....	8-2
8-3	RMON Statistics Screen .....	8-4
8-4	Unicast Address Table Screen .....	8-7
8-5	IP Multicast Registration Table Screen .....	8-8
9-1	System Restart Menu Screen .....	9-1
A-1	Spanning Tree Using Switches .....	A-2
B-1	Example of Multi-Switch VLAN Configuration .....	B-3
C-1	Class of Service Example .....	C-2

---

# Tables

Table		Page
2-1	VT Terminal Setup.....	2-3
3-1	Factory Default Settings .....	3-5
7-1	SmartTrunk, Ports Associated with Group IDs .....	7-21
10-1	SmartTrunk Configuration, Ports Associated with Group IDs.....	10-12
A-1	Spanning Tree Protocol Defaults.....	A-3



---

# About This Guide

Welcome to the Enterasys Networks<sup>®</sup>™ **MATRIX E5 Series Modules (5H1xx and 5G1xx) Local Management User's Guide**. This manual explains how to access and use the Local Management screens to monitor and manage 5H1xx and 5G1xx modules, attached segments, in a five-slot 5C105 chassis. Only the 5H1xx and 5G1xx modules can operate in the 5C105 chassis.

---

## Important Notice

Depending on the firmware version used in the module, some features described in this document may not be supported. Refer to the Release Notes shipped with the module to determine which features are supported.

---

## USING THIS GUIDE

A general working knowledge of basic network operations and an understanding of management applications is helpful prior to using Local Management.

This manual describes how to do the following:

- Access the Local Management application
- Identify and operate the types of fields used by Local Management
- Navigate through Local Management fields and menus
- Use Local Management screens to perform management operations
- Establish and manage Virtual Local Area Networks (VLANs)

## STRUCTURE OF THIS GUIDE

The guide is organized as follows:

Chapter 1, **Introduction**, provides an overview of the tasks that may be accomplished using Local Management (LM), and an introduction to LM screen navigation, in-band and out-of-band network management. This chapter also contains information on how to get help from Enterasys Networks if needed.

Chapter 2, **Local Management Requirements**, provides the setup requirements for accessing Local Management and the instructions to configure and connect a management terminal to the module.

Chapter 3, **Accessing Local Management**, describes how to navigate through the screen hierarchy and access the Password screen to enter a Local Management session. The default parameter settings for each screen are also provided.

Chapter 4, **Main Menu Screens**, describes the Main Menu screen, introduces the screens that you can use to obtain system operating information, change operating parameters, obtain module operating statistics, reset and exit Local Management. The Main Menu screen is the access point to the top level screens of Local Management.

Chapter 5, **System Information Menu Screens**, describes the System Information Menu screen and the two screens that can be selected from its menu. These screens are used to display a basic description of the module, including contact information, hardware/firmware versions and the chassis slot that the module is occupying.

Chapter 6, **Management Setup Menu Screens**, describes how to access and use the screens that enable you to adjust the communication parameters for your console, specify the IP addresses for the module, set the Administrator and User passwords, and set the community string, which controls access to the on-board SNMP agent via in-band management software.

Chapter 7, **Device Control Menu Screens**, describes how to access and use the screens that enable you to control a broad range of functions, including port configuration, Spanning Tree support for redundant switches, port mirroring, multicast filtering, and Virtual LANs.

Chapter 8, **Network Monitoring Menu Screens**, describes how to access the switch port statistics, RMON statistics, IP multicast addresses, and the static (unicast) address table.

Chapter 9, **System Restart Menu Screen**, enables you to run the Power-On Self-Test, reload the factory defaults, retain the settings defined in the IP Configuration menu, and retain the user names and passwords defined in the Console Login Configuration menu.

Chapter 10, **Configuring and Monitoring the Switch**, describes the common tasks in setting up and operating the switch using the Local Management (LM) screens. The LM screens allow you to modify the default switch settings and configure the switch for network management. The LM screens also allow you to monitor the switch performance and status.

Chapter 11, **SNMP Management**, introduces you to SNMP (Simple Network Management Protocol), which is a communication protocol for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, routers, and host computers.



Appendix A, **Spanning Tree Concepts**, introduces you to the IEEE 802.1D Spanning Tree Protocol. This protocol is used to resolve the problems of physical loops in a network by establishing one primary path between any two switches in a network.

Appendix B, **System Restart Menu Screen**, introduces you to IEEE 802.1Q-compliant virtual LANs (VLANs). This capability provides a highly efficient architecture for establishing VLANs within a network and for controlling broadcast/multicast traffic between workgroups.

Appendix C, **Class of Service**, introduces you to the Class of Service capability, which is based on the IEEE 802.1p standard specification. This capability allows you to assign mission-critical data to a higher priority through the switch by delaying less critical traffic during periods of congestion. Higher priority traffic through the switch is serviced first before lower priority traffic.

Appendix D, **IP Multicast Filtering**, introduces you to the Internet Group Management Protocol (IGMP). This protocol runs between hosts and their nearest neighboring multicast router/switch. The protocol's mechanisms allow a host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

## RELATED DOCUMENTS

The following Enterasys Networks document may help to set up, control, and manage the module:

- *5C105 MATRIX E5 Overview and Setup Guide*

This document along with other Enterasys Networks documents can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

<http://www.enterasys.com>

## DOCUMENT CONVENTIONS

The guide uses the following conventions:



**NOTE:** Calls the reader's attention to any item of information that may be of special importance.



**TIP:** Conveys helpful hints concerning procedures or actions.



**CAUTION:** Contains information essential to avoid damage to the equipment.

## TYPOGRAPHICAL AND KEYSTROKE CONVENTIONS

<b>bold type</b>	Bold type can denote either a user input or a highlighted screen selection.
ENTER	Indicates either the ENTER or RETURN key, depending on your keyboard.
ESC	Indicates the keyboard Escape key.
SPACE bar	Indicates the keyboard space bar key.
BACKSPACE	Indicates the keyboard backspace key.
arrow keys	Refers to the four keyboard arrow keys.
[-]	Indicates the keyboard – key.
DEL	Indicates the keyboard delete key.
<i>italic type</i>	Italic type indicates complete document titles.
n.nn	A period in numerals signals the decimal point indicator (e.g., 1.75 equals one and three fourths). Or, periods used in numerals signal the decimal point in Dotted Decimal Notation (DDN) (e.g., 000.000.000.000 in an IP address).
<i>x</i>	A lowercase italic <i>x</i> indicates the generic use of a letter (e.g., <i>xxx</i> indicates any combination of three alphabetic characters).
<i>n</i>	A lowercase italic <i>n</i> indicates the generic use of a number (e.g., 19 <i>nn</i> indicates a four-digit number in which the last two digits are unknown).
[ ]	In the Local Management screens, the square brackets indicate that a value may be selected. In the format descriptions in the Network Tools section, required arguments are enclosed in square brackets, [ ].
< >	In the format descriptions in the Network Tools section, optional arguments are enclosed in angle brackets, < >.

---

## GETTING HELP

For additional support related to this product or document, contact Enterasys Networks using one of the following methods:

---

World Wide Web	<a href="http://www.enterasys.com">http://www.enterasys.com</a>
Phone	(603) 332-9400
Internet mail	<a href="mailto:support@enterasys.com">support@enterasys.com</a>
FTP	<a href="ftp://ftp.enterasys.com">ftp://ftp.enterasys.com</a>
Login	<i>anonymous</i>
Password	<i>your email address</i>

---

To send comments or suggestions concerning this document, contact the Enterasys Networks Technical Writing Department via the following email address: **TechWriting@enterasys.com**

Make sure to include the document Part Number in the email message.

---

### **Before calling Enterasys Networks, have the following information ready:**

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers



---

# Introduction

This chapter provides an overview of the tasks that may be accomplished using Local Management (LM), and an introduction to LM screen navigation, in-band and out-of-band network management, screen elements, and LM keyboard conventions.

---

## Important Notice

Depending on the firmware version used in the switch module, some features described in this document may not be supported. Refer to the Release Notes shipped with the switch module to determine which features are supported.

---

## 1.1 OVERVIEW

The switch module provides a menu-driven system configuration program referred to as Local Management. This program can be accessed by a direct or modem connection to the COM port on the switch module (out-of-band), or by a Telnet connection over the network (in-band).

The Local Management is based on SNMP (Simple Network Management Protocol). This SNMP agent permits a switch to be managed from any PC in the network using in-band management software.

The switch module also includes an embedded HTTP Web agent. This Web agent can be accessed using a standard Web browser from any computer attached to the network.

The system configuration program and the SNMP agent support management functions such as:

- Enable/disable any port
- Set the communication mode for any port
- Configure SNMP parameters
- Select RMON options
- Display system information or statistics
- Configure the switch to join a Spanning Tree

- Download system firmware
- Restart the system

There are three ways to access Local Management:

- Locally using a VT type terminal connected to the COM port.
- Remotely using a VT type terminal connected through a modem.
- In-band through a Telnet connection.

### 1.1.1 The Management Agent

The management agent is an entity within the switch module that collects statistical information (e.g., frames received, errors detected) about the operational performance of the managed network. Local Management communicates with the management agent for the purpose of viewing statistics or issuing management commands. Local Management provides a wide range of screens used to monitor and configure the switch module.

### 1.1.2 In-Band vs. Out-of-Band

Network management systems are often classified as either in-band or out-of-band. In-band network management passes data along the same medium (cables, frequencies) used by all other stations on the network. An example of an in-band network management system is the Enterasys Networks NetSight™.

Out-of-band network management passes data along a medium that is entirely separate from the common data carrier of the network, for example, a cable connection between a terminal and a switch module COM port. Enterasys Networks' Local Management is an out-of-band network management system.

A module connected out-of-band to the management agent is not connected to the LAN. This type of connection allows you to communicate with a network module even when that module is unable to communicate through the network, for example, at the time of installation.

## 1.2 NAVIGATING LOCAL MANAGEMENT SCREENS

To navigate within a Local Management screen, use the arrow keys of the terminal or the workstation providing terminal emulation services. The Local Management screen cursor responds to the LEFT, RIGHT, UP, and DOWN arrow keys. Each time you press an arrow key, the Local Management screen cursor moves to the next available field in the direction of the arrow key.

The Local Management screen cursor only moves to fields that can be selected or used for input. This means that the cursor jumps over display fields and empty lines on the Local Management screen.

The Local Management screen cursor provides wrap-around operation. This means that a cursor located at the edge of a screen, when moved in the direction of that edge, “wraps around” to the outermost selectable item on the opposite side of the screen which is on the same line or column.

## 1.3 LOCAL MANAGEMENT REQUIREMENTS

The switch module provides one communication port, labeled COM, which supports a management terminal connection. To access Local Management, connect one of the following systems to the COM port:

- Digital Equipment Corporation VT series terminal.
- VT type terminal running emulation programs for the Digital Equipment Corporation VT series.
- IBM or compatible PC running a VT series emulation software package such as Hyperterm, which is included in the Windows 9x operating system.

You can also access Local Management using a Telnet connection through one of the network ports of the switch module.



**NOTE:** For details on the setup parameters for the console, how to connect a console to the switch module, or how to make a telnet connection, refer to [Chapter 2](#).





---

## Local Management Requirements

To change the operating parameters of the module, you must access its Local Management program by either a module COM port connection or by a Telnet connection to the module. This chapter provides the following sections on how to make these connections:

- Management Terminal Setup ([Section 2.1](#)), which describes how to make a terminal connection to the module COM port.
- Telnet Connection ([Section 2.2](#)), which provides guidelines on how to make a Telnet connection to access Local Management.

### 2.1 MANAGEMENT TERMINAL SETUP

The switch module provides one communication port, labeled COM, which supports a management terminal connection. To access Local Management, connect one of the following systems to the COM port:

- Digital Equipment Corporation VT series terminal.
- VT type terminal running emulation programs for the Digital Equipment Corporation VT series.
- IBM or compatible PC running a VT series emulation software package such as Hyperterm, which is included in the Windows 9x operating system.
- You can also access Local Management using a Telnet connection through one of the network ports of the switch module.

#### 2.1.1 Console Cable Connection

Use the Console Cable Kit provided with the switch module to attach the management terminal to the switch module COM port as shown in [Figure 2-1](#).

To connect the switch module to a PC or compatible device running the VT terminal emulation, proceed as follows:

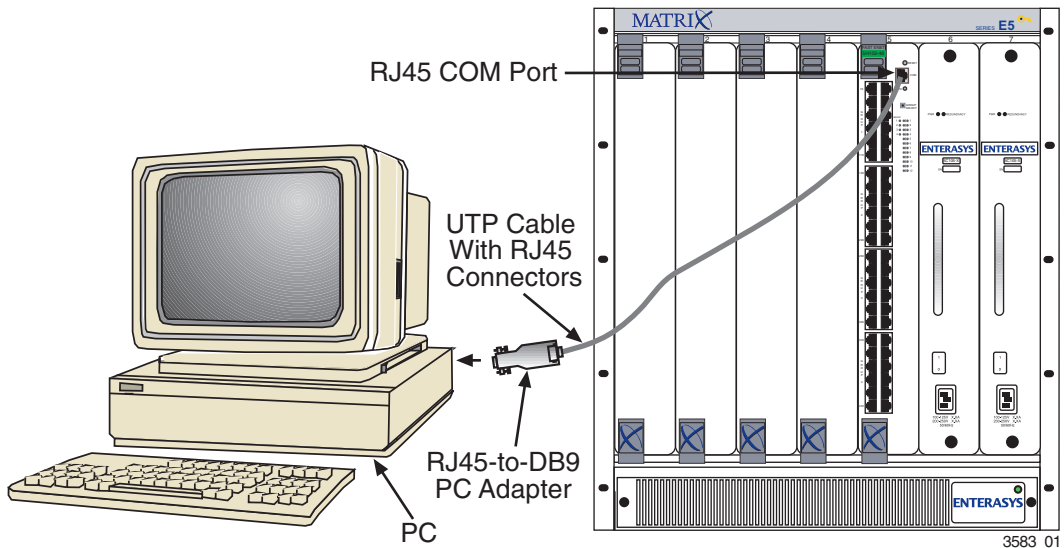
1. Connect the RJ45 connector at one end of the cable (supplied in the kit) to the COM port on the switch module.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 adapter (supplied in the kit).
3. Connect the RJ45-to-DB9 adapter to the PC communications port.



**NOTE:** If using a modem between the VT compatible device and the COM port of the switch module, use the appropriate connector included in the console cable kit. Refer to the modem manufacturer's information for proper operation and setup of the modem.

The 5H102-48 module is shown in [Figure 2-1](#) as an example.

**Figure 2-1 Management Terminal Connection**



### 2.1.2 Management Terminal Setup Parameters

[Table 2-1](#) lists the setup parameters for the local management terminal.

Table 2-1 VT Terminal Setup

Parameter	Setting
<b>Display Setup Menu</b>	
Columns ->	80 Columns
Controls ->	Interpret Controls
Auto Wrap ->	No Auto Wrap
Scroll ->	Jump Scroll
Text Cursor ->	Cursor
Cursor Style ->	Underline Cursor Style
<b>General Setup Menu</b>	
Mode ->	VT100, 7 Bit Controls
ID number ->	VT100ID
Cursor Keys ->	Normal Cursor Keys
Power Supply ->	UPSS DEC Supplemental
<b>Communications Setup Menu</b>	
Transmit ->	2400, 4800, 9600, 19200 (Recommended setting is 9600, which is the default when the switch boots up.)
Receive ->	Receive=Transmit
XOFF ->	XOFF at 64
Bits ->	8 bits
Parity ->	No Parity
Stop Bit ->	1 Stop Bit
Local Echo ->	No Local Echo
Port ->	DEC-423, Data Leads Only
Transmit ->	Limited Transmit
Auto Answerback ->	No Auto Answerback
<b>Keyboard Setup Menu</b>	
Keys ->	Typewriter Keys
Auto Repeat ->	any option
Keyclick ->	any option
Margin Bell ->	Margin Bell
Warning Bell ->	Warning Bell

## 2.2 TELNET CONNECTIONS

Prior to accessing a module via a network connection, you must first configure the module with a valid IP address, subnet mask, and default gateway using an out-of-band connection or the BOOTP protocol.

Once the switch module is configured, you can establish a Telnet session from any TCP/IP based node on the network. Telnet connections to the switch module require the community name passwords assigned in the SNMP Configuration screen.

For information about setting the IP address, refer to [Chapter 6](#).

For information about assigning community names, refer to [Chapter 6](#).

Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

---

## Accessing Local Management

To provide you with an overall awareness of the Local Management screens used to configure the module and the default settings for each parameter, this chapter provides information about the following:

- Navigating through the Local Management hierarchy. A flowchart provides a quick overview of the menu screens and their subordinate screens ([Section 3.1](#)). You are also introduced to the types of information displayed on a screen, and how to use the cursor to navigate to various screen fields to select menu items and make parameter changes.
- Description of a typical screen layout and how to use the menu items to access other screens ([Section 3.2](#)).
- Accessing the Password screen to enter a Local Management session ([Section 3.3](#)).
- The default settings for each switch configuration parameter. These are the parameters that can be changed via a terminal connected to the COM port of the module or a Telnet session [Section 3.4](#).

---

### Important Notice

Depending on the firmware version used in the switch module, some features described in this document may not be supported. Refer to the Release Notes shipped with the switch module to determine which features are supported.

---

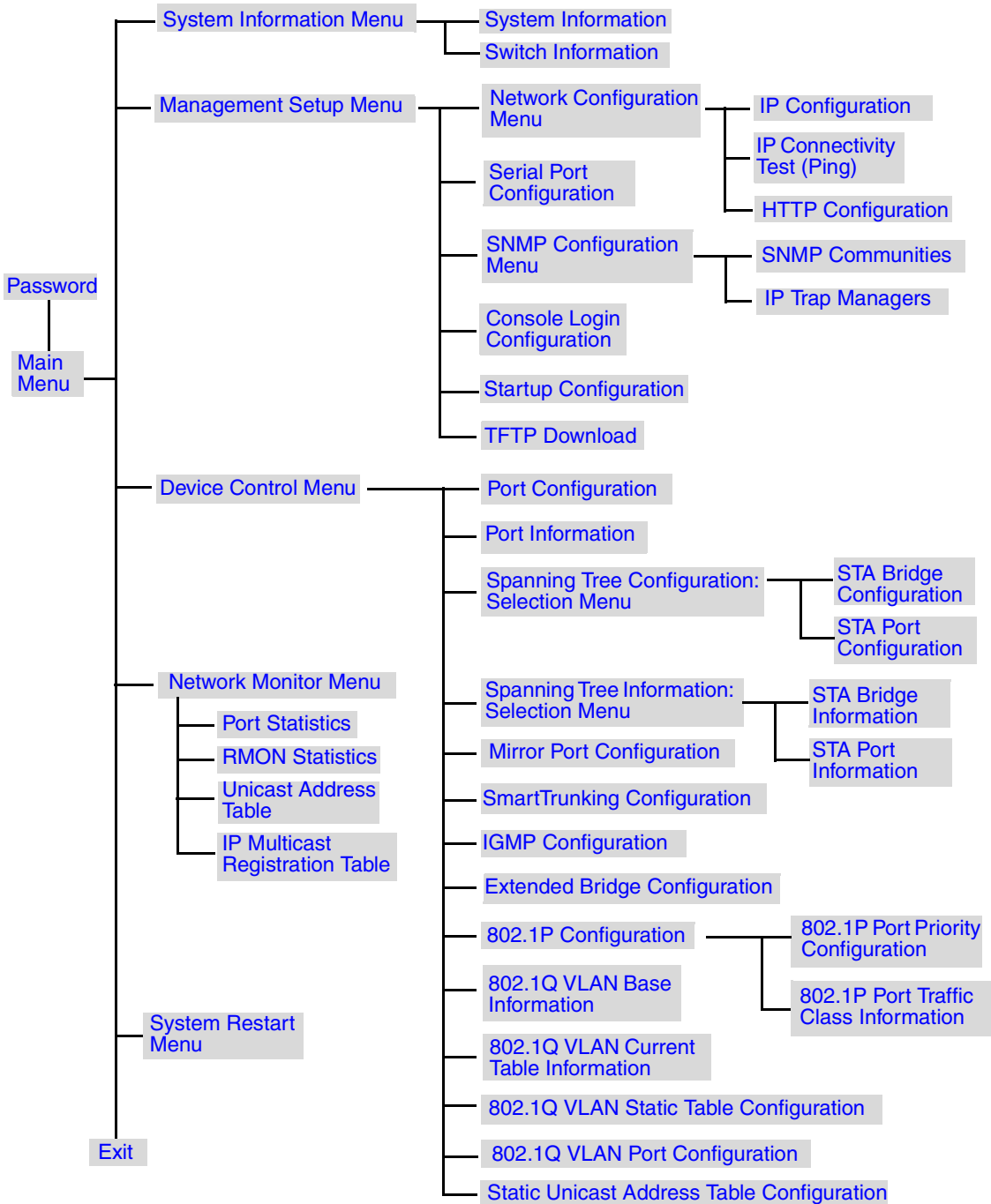
### 3.1 NAVIGATING LOCAL MANAGEMENT SCREENS

The switch module Local Management application consists of a series of menu screens. Navigate through Local Management by selecting items from the menu screens. [Figure 3-1](#) shows the hierarchy of the Local Management screens.



**NOTE:** At the beginning of each chapter, a section entitled “Screen Navigation Path” shows the navigation path to the first screen described in the chapter.

Figure 3-1 Local Management Screen Hierarchy

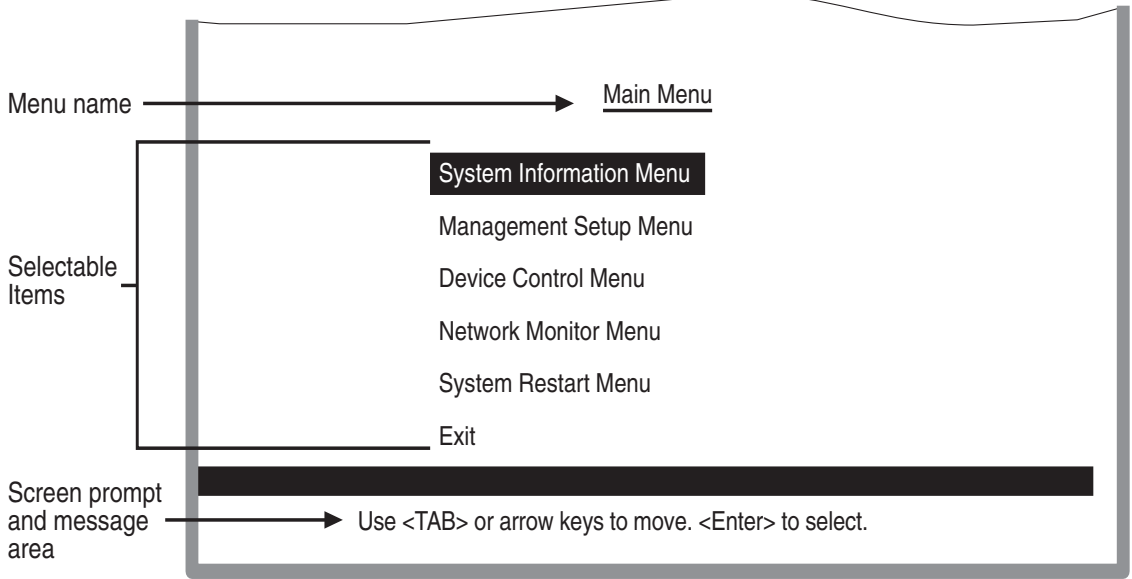


### 3.2 ACCESSING LOCAL MANAGEMENT SCREENS

Access to the Local Management screens menus is gained by connecting a terminal to the console port through a direct cable connection or over a modem, or using Telnet to access the Local Management over the network as detailed in [Chapter 2](#). The menus allow you to reconfigure the module, as well as to monitor its status and performance. The menus have a layout similar to the sample Main Menu shown in [Figure 3-2](#). The information is divided into the following parts:

- Menu Name (includes access privileges)
- Selectable Items
- Screen Prompt for menu selections and entry of field parameters, and Message Area for the display of parameters or error messages

**Figure 3-2 Sample Main Menu**



3583\_03



**NOTE:** A table following the figure of each screen provides a functional description of each field on that screen.

## How to Use the Screen Menus

To use the screen menus, do the following:

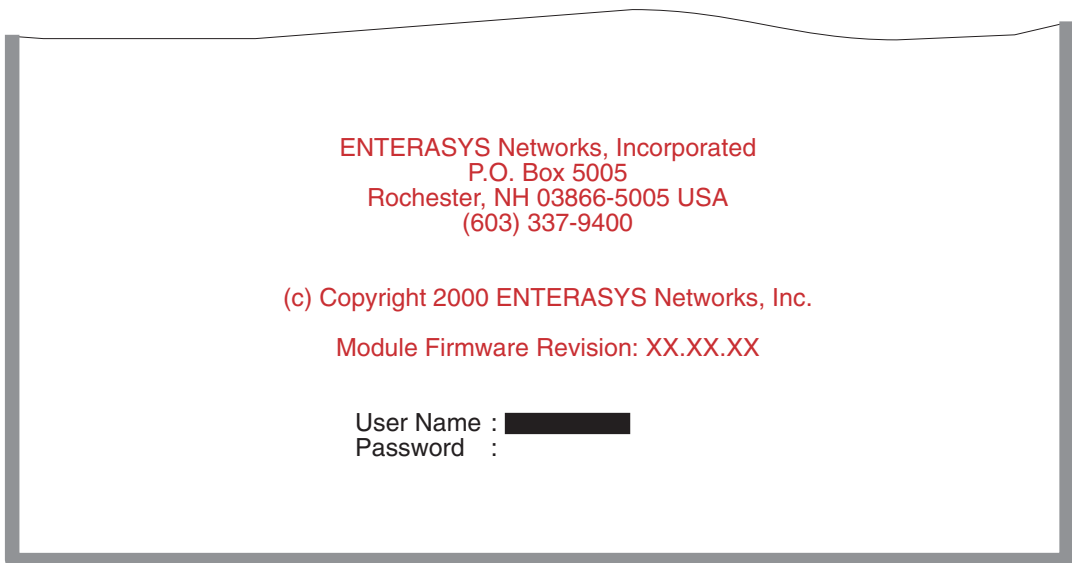
1. Use the cursor keys to highlight the desired option. If the selected item is a submenu title, the submenu is displayed when you press the ENTER key.
2. Follow the screen prompts to specify the parameter requested.

If the selected item is a parameter, the system displays a prompt for you to enter a new value. If the value entered is invalid, a message displays, requesting you to enter a valid value.

## 3.3 PASSWORD SCREEN

Once a direct connection to the serial port or a Telnet connection is established, the login Password screen (Figure 3-3) for the on-board Local Management configuration program displays.

**Figure 3-3 Password Screen**



3583\_04

You may need to press ENTER a few times to display the screen. The default user name is “public,” with no passwords. The administrator has Read/Write access, which allows you to read and modify switch information. The guest has Read Only access to the management program, which allows you to view switch information, but not modify any operating parameters.



You should assign a new administrator password, record it and put it in a safe place for future reference.

To assign a new password, start at the Main Menu, select Management Setup Menu /Console Login Configuration, and enter a new password for the administrator. Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.



**NOTE:** A user is allowed three attempts to enter the correct password; on the third failed attempt, the current connection is terminated.

### 3.4 FACTORY DEFAULTS

Table 3-1 lists the default settings for switch configuration parameters. Each parameter can be changed via the console menus or Telnet.

**Table 3-1 Factory Default Settings**

Parameter	Default Value
Multicast Filtering	
IGMP Multicast Filtering	Disabled
Port Configuration	
Speed and Duplex	Auto
Admin	Enabled
Port Priority	
Default Ingress User Priority	0

**Table 3-1 Factory Default Settings (Continued)**

<b>Parameter</b>	<b>Default Value</b>
<b>Spanning Tree Algorithm</b>	
Active Aging Time	300
Bridge Priority	32768
Forward Delay	15
Hello Time	2
Max Age	20
Path Cost	4 - 1000 Mbps ports 9 - 100 Mbps ports 100 - 10 Mbps ports
Port Priority	128
Spanning Tree Protocol	Enabled
<b>System Configuration</b>	
Password	<none>
Screen Time-out	10 minutes
Send Authentication Fail Traps	Enabled
SNMP Community Names	Public, private
Terminal Baud Rate	9600
User Name	public
<b>Virtual LANs</b>	
Acceptable VLAN Frame Type	All
Configurable PVID Tagging	Yes
Untagged VLAN Group Assignment	1
VLAN Ingress Filtering	False
VLAN Learning	SVL
Auto Backplane VLAN Configuration	Yes

---

---

## Main Menu Screens

Once you have logged into Local Management, the Main Menu screen is the first screen to display. This chapter describes the Main Menu screen, introduces the screens that you can use to obtain system operating information, change operating parameters, obtain module operating statistics, reset and exit Local Management.

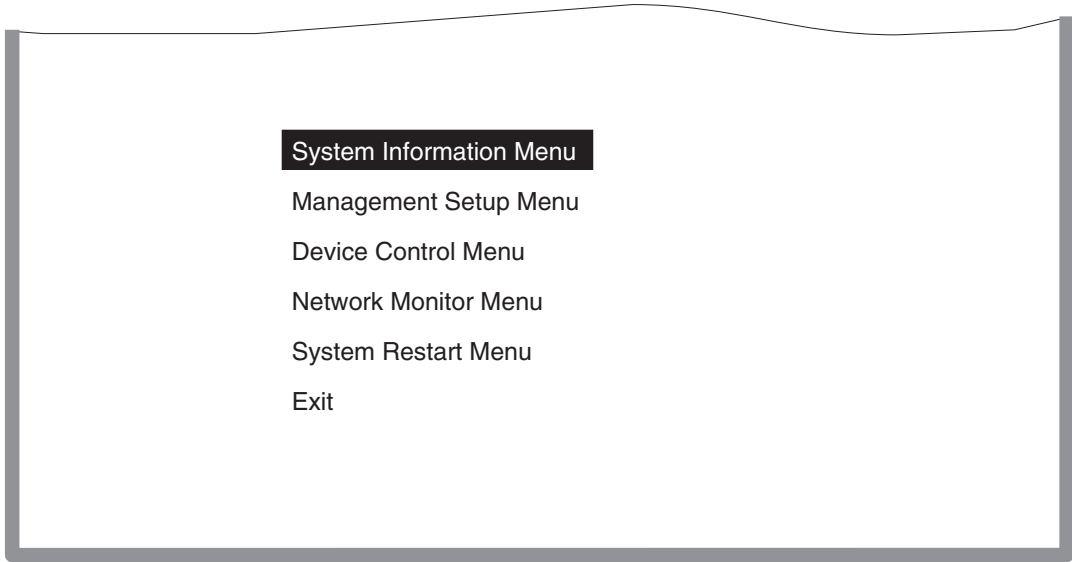
### Screen Navigation Path

Password > **Main Menu**

## 4.1 MAIN MENU

The Main Menu screen provides access to the five top level menu screens and the EXIT command, which is used to end a Local Management session. The Main Menu screen ([Figure 4-1](#)) and the reporting screen functions are described below.

**Figure 4-1 Main Menu**



3583\_05

Selection	Description
<b>System Information Menu (For details, refer to <a href="#">Chapter 5</a>.)</b>	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the chassis.

---

Selection	Description
<b>Management Setup Menu (For details, refer to <a href="#">Chapter 6.</a>)</b>	
Network Configuration Menu	Includes IP setup, Ping facility, HTTP (Web Agent) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration Menu	Activates traps and configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download	Downloads new version of firmware to update your system (in-band).
<b>Device Control Menu (For details, refer to <a href="#">Chapter 7.</a>)</b>	
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Port Information	Displays operational status, including link state, flow control method, and duplex mode.
Spanning Tree Configuration	Enables Spanning Tree Algorithm; also sets parameters for hello time, maximum message age, switch priority, and forward delay; as well as port priority and path cost.
Spanning Tree Information	Displays full listing of parameters for the Spanning Tree Algorithm.
Mirror Port Configuration	Sets the source and target ports for mirroring.
SmartTrunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.

---

Selection	Description
<b>Device Control Menu (Cont'd)</b>	
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, and VLAN extensions.
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, and ingress filtering.
Static Unicast Address Table Configuration	Used to manually configure host MAC addresses in the unicast table.
<b>Network Monitor Menu (For details, refer to <a href="#">Chapter 8</a>.)</b>	
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full address listing, as well as search and clear functions.
IP Multicast Registration Table	Displays all the multicast groups active on this switch, including multicast IP addresses and corresponding VLAN IDs.
<b>System Restart Menu (For details, refer to <a href="#">Chapter 9</a>.)</b>	
	Restarts system with options to use POST, or to retain factory defaults, IP settings, or user authentication settings.
<b>Exit (For details, refer to <a href="#">Chapter 9</a>.)</b>	
	Exits the configuration program.

---

# System Information Menu Screens

This chapter describes the System Information Menu screen and the screens that can be selected from its menu to obtain system and switch information.

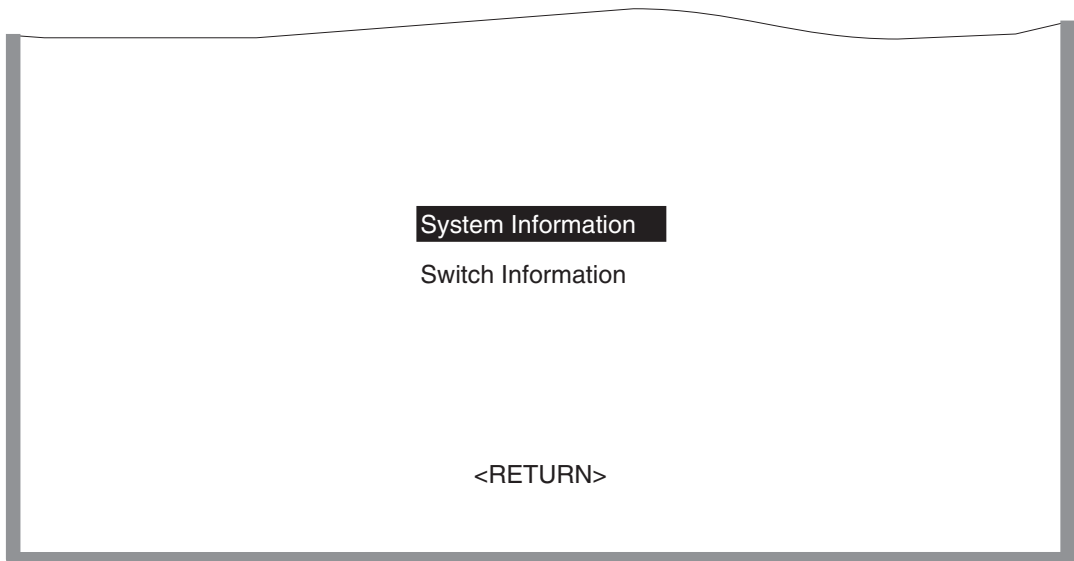
## Screen Navigation Path

Password > Main Menu > **System Information Menu**

### 5.1 SYSTEM INFORMATION MENU SCREEN

Use the System Information Menu screen (Figure 5-1) described below to access the System Information and Switch Information screens to display a basic description of the switch, including contact information, and hardware/firmware versions.

**Figure 5-1 System Information Menu Screen**



3583\_06

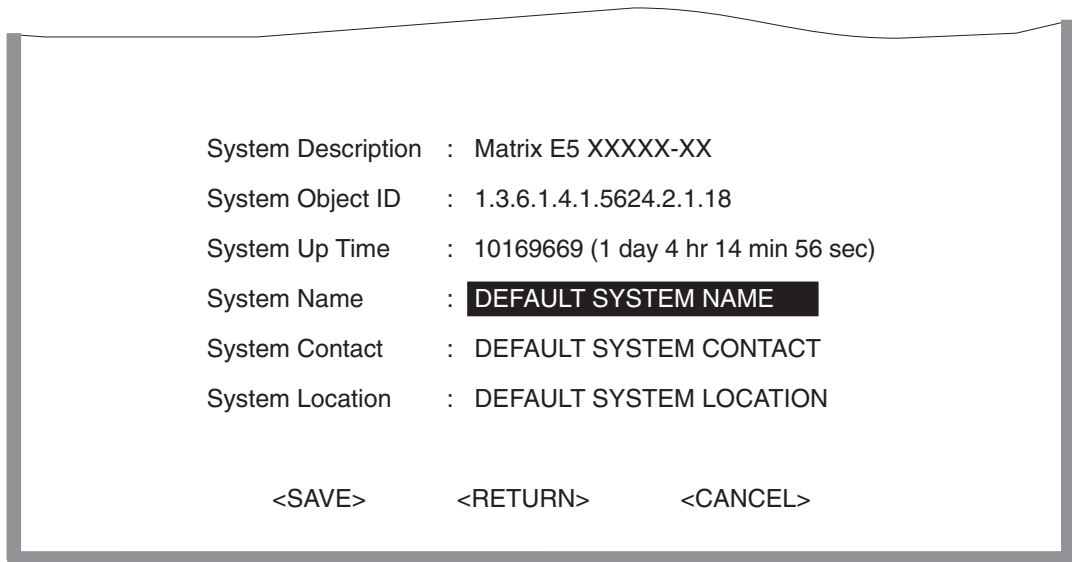
Selection	Description
System Information	Provides basic system description, including system object ID, up time, name, contact, and location.
Switch Information	Shows hardware/firmware version numbers, serial number, and number of the chassis slot being occupied by the module.

---

### 5.1.1 Displaying System Information

Use the System Information screen (Figure 5-2) described below to display descriptive information about the switch, or for quick system identification.

**Figure 5-2 System Information Screen**



3583\_07



---

<b>Parameter</b>	<b>Description</b>
System Description	System hardware description.
System Object ID	MIB II object identifier for switch is network management subsystem.
System Up Time	Length of time the current management agent has been running. (Note that the first value is 1/100 seconds.)
System Name *	Name assigned to the switch system.
System Contact *	Contact person for the system.
System Location *	Specifies the area or location where the system resides.

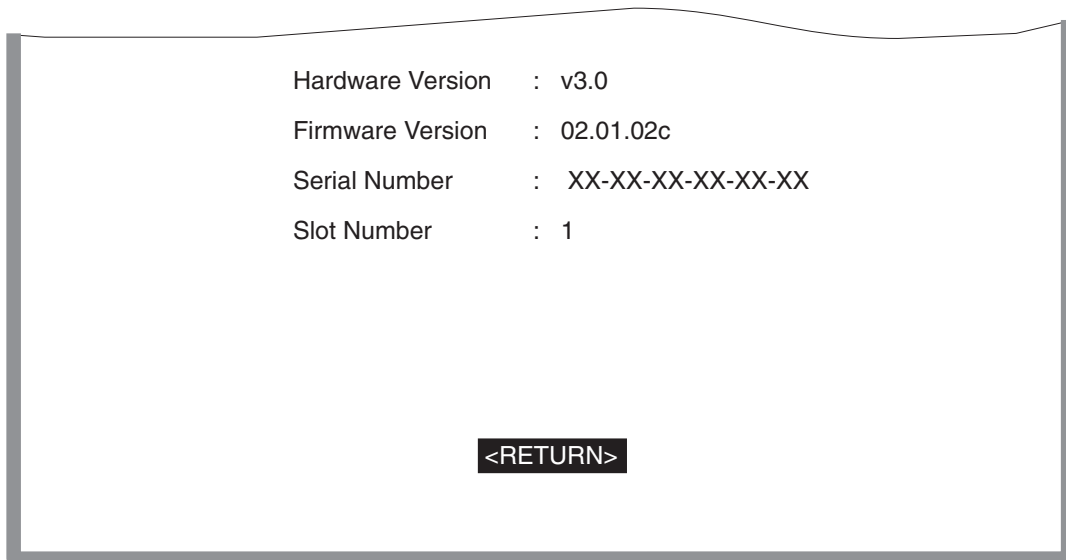
---

\* Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

## 5.1.2 Displaying Switch Version and Module Information

Use the Switch Information screen (Figure 5-3) described below to display the module hardware/firmware version numbers, serial number and slot number it occupies in the chassis.

**Figure 5-3 Switch Information Screen**



3583\_08

Parameter	Description
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	MAC address associated with the main board.
Slot Number	Number of the Chassis Slot occupied by the module.

---

## Management Setup Menu Screens

The Management Setup Menu screen provides access to the screens used to set up the console communications parameters and specify the switch IP address, passwords to Local Management screens, and switch SNMP configuration.

After initially logging onto the system, perform the following:

- Adjust the communication parameters for your console to ensure a reliable connection (Serial Port Configuration). Refer to [Section 6.3](#).
- Specify the IP address for the module (Network Configuration / IP Configuration). Refer to [Section 6.2](#).
- Set the Administrator and User passwords (Console Login Configuration). Refer to [Section 6.5](#). Remember to record the passwords and keep them in a safe place.
- Set the community string, which controls access to the on-board SNMP agent via in-band management software (SNMP Configuration). Refer to [Section 6.4](#).

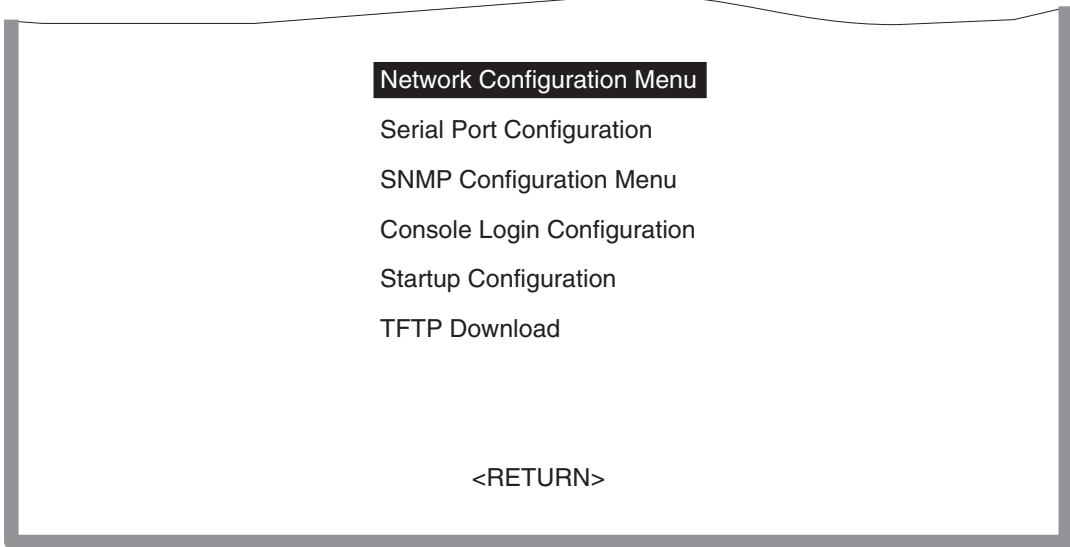
### Screen Navigation Path

Password > Main Menu > **Management Setup Menu**

## 6.1 MANAGEMENT SETUP MENU SCREEN

The menu items provided by the Management Setup Menu screen ([Figure 6-1](#)) are described in the following sections.

**Figure 6-1 Management Setup Menu Screen**



3583\_09

Selection	Description
Network Configuration Menu	Provides access to two screens to perform functions that include IP setup, Ping facility, HTTP (Web Agent) setup, Telnet configuration, and MAC address. For details, refer to <a href="#">Section 6.2</a> .
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval. For details, refer to <a href="#">Section 6.3</a> .
SNMP Configuration Menu	Activates traps and configures communities and trap managers. For details, refer to <a href="#">Section 6.4</a> .
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time. For details, refer to <a href="#">Section 6.5</a> .

Selection	Description
Startup Configuration	Used to disable the extended system diagnostics during system bootup routine for faster bootups. For details, refer to <a href="#">Section 6.6</a> .
TFTP Download	Downloads new version of firmware to update your system (in-band). For details, refer to <a href="#">Section 6.7</a> .

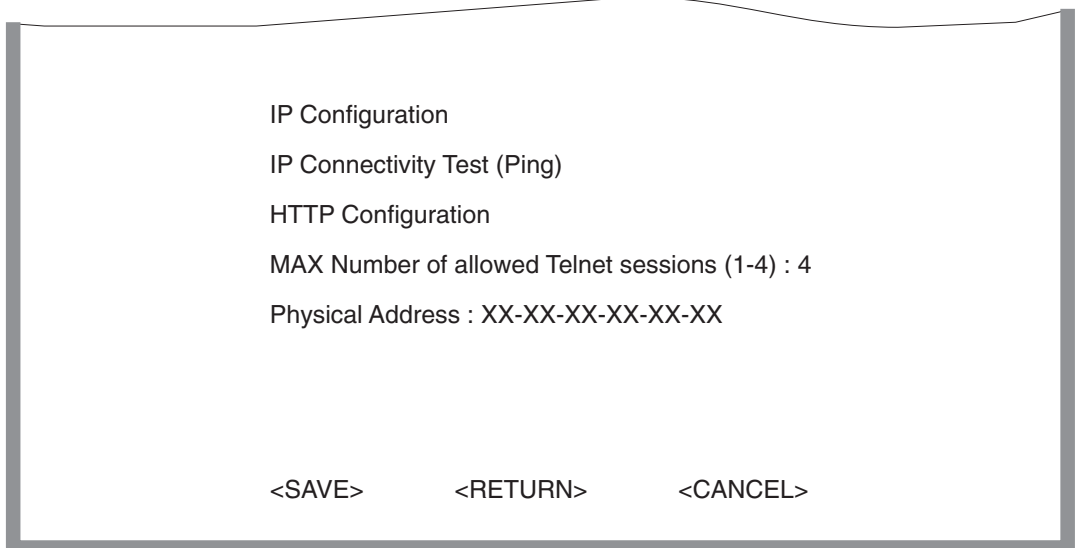
## 6.2 CHANGING THE NETWORK CONFIGURATION

Use the Network Configuration Menu screen ([Figure 6-2](#)) for any of the following:

- Access the screens needed to set the bootup option.
- Configure the switch’s Internet Protocol (IP) parameters.
- Enable the on-board Web Agent.
- Set the number of concurrent Telnet sessions allowed.

The screen shown below is described in the following table.

**Figure 6-2 Network Configuration Menu Screen**



3583\_10

Parameter	Description
IP Configuration	Used to set the bootup option, or configure the switch's IP parameters.
IP Connectivity Test (Ping)	Used to test IP connectivity (Ping) to a specified device.
HTTP Configuration	Used to enable the Web Agent.
MAX Number of Allowed Telnet Sessions (1-4)	The maximum number of Telnet sessions allowed to simultaneously access the agent module.
Physical Address	Physical address of the agent module.

## 6.2.1 IP Configuration

Use the IP Configuration screen (Figure 6-3) to set the bootup option, or configure the switch's IP parameters. The screen shown below is described in the following table.

**Figure 6-3 IP Configuration Screen**

```
Interface Type      : Ethernet
IP Address         : XXX.XXX.XXX.XXX
Subnet Mask        : XXX.XXX.XX.XX
Gateway IP         : XXX.XXX.XX.X
IP State           : USER-CONFIG

<SAVE>            <RETURN>            <CANCEL>
```

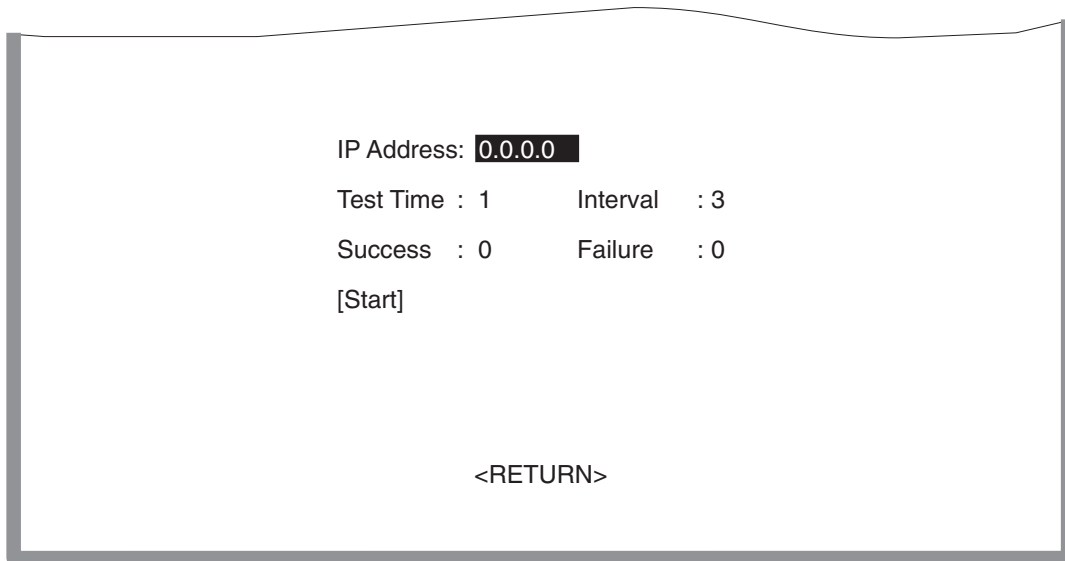
3583\_11

Parameter	Default	Description
Interface Type	Ethernet	Indicates IP over Ethernet.
IP Address	0.0.0.0.	IP address of the module you are managing when accessing the agent module over the network. The agent module supports SNMP over UDP/ IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module (or running NetSight) must have an IP address. Valid IP addresses consist of four numbers, from 0 to 255, that are separated by periods ( <i>nnn.nnn.nnn.nnn</i> ). Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255. 0.0	Subnet mask of the agent you have selected. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP	0.0.0.0	Gateway used to pass trap messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
IP State	USER-CONFIG	<p>Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include</p> <p>USER-CONFIG — The IP functionality is enabled based on the default or user-specified IP Configuration, which is the default.</p> <p>BOOTP Get IP — The IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, subnet mask, TFTP boot file name, and TFTP server IP.)</p>

## 6.2.2 IP Connectivity Test (Ping)

Use the IP Connectivity Test screen (Figure 6-4) to see if another site on the Internet can be reached. The screen parameters are described in the following table.

Figure 6-4 IP Connectivity Test Screen



3583\_12

Parameter	Description
IP Address	IP address of the site that you want to ping.
Test Time	The number of ICMP echo requests to send to the specified site. Range: 1~1000
Interval	The interval (in seconds) between pinging the specified site. Range: 1~10 seconds
Success/Failure	The number of times the specified site has or has not responded to pinging.
[Start] command	This field is used to initiate the ping. To ping an address, highlight [Start] using the arrow keys, then press ENTER.



### 6.2.3 HTTP Configuration

Use the HTTP Configuration screen (Figure 6-5) to enable/disable the on-board Web agent, and to specify the TCP port that will provide HTTP service. The screen shown below is described in the following table.

**Figure 6-5 HTTP Configuration Screen**

HTTP Server : **ENABLED**

HTTP Port Number : 80

<SAVE>                      <RETURN>                      <CANCEL>

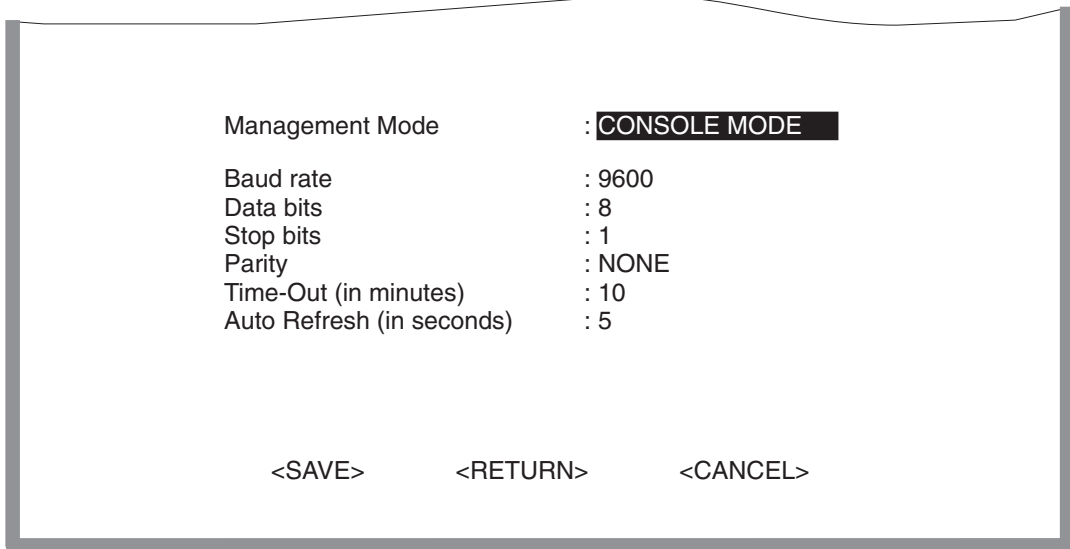
3583\_13

Parameter	Description
HTTP Server	Enables/disables access to the on-board web agent for WebView.
HTTP Port Number	Specifies the TCP port that will provide HTTP service. Range: 0~65535 Default: Port 80 (Telnet Port 23 is prohibited.)

### 6.3 CONFIGURING THE SERIAL PORT

You can access the on-board configuration program by attaching a VT100 compatible device to the switch's COM port. (For more information on connecting to this port, refer to [Chapter 2](#).) The communication parameters for this port can be accessed from the Serial Port Configuration screen ([Figure 6-6](#)) shown below and described in the following table.

**Figure 6-6 Serial Port Configuration Screen**



3583\_14

---

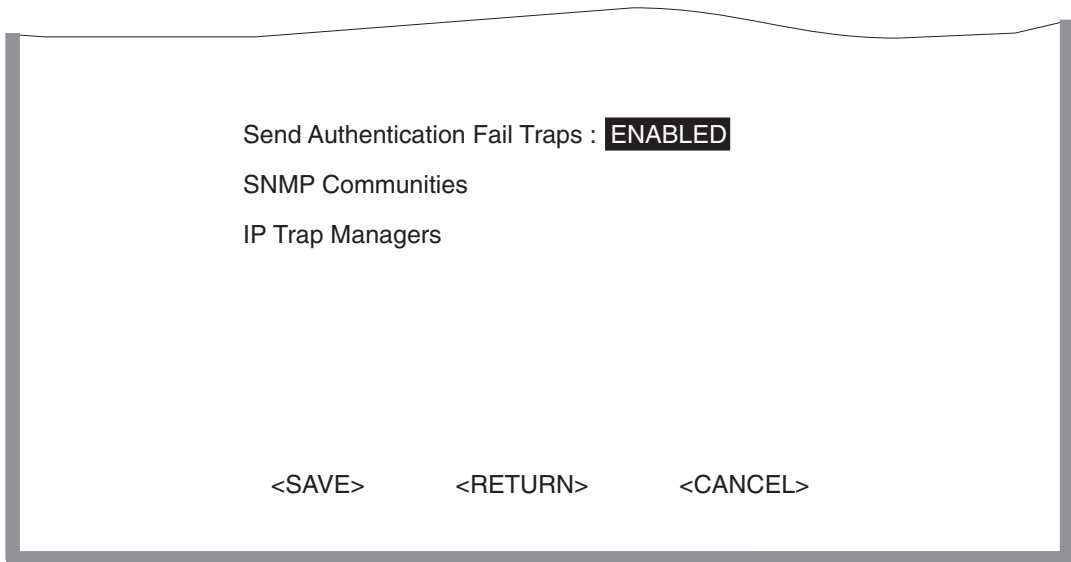
Parameter	Default	Description
Management Mode	CONSOLE MODE	Indicates that the console port settings are for direct console connection.
Baud rate	9600	The rate at which data is sent between devices. Options: 2400, 4800, 9600, and 19200 bps.
Data bits	8 bits	Sets the data bits of the RS232 port. Options: 7, 8
Stop bits	1 bit	Sets the stop bits of the RS232 port. Options: 1, 2
Parity	NONE	Sets the parity of the RS232 port. Options: none/odd/even
Time-Out (in minutes)	10	If no input is received from the attached device after this interval, the current session is automatically closed. Range: 0-100 minutes; 0: disabled
Auto Refresh (in seconds)	5	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range: 5-255 seconds; 0: disabled

---

## 6.4 ASSIGNING SNMP PARAMETERS

Use the SNMP Configuration Menu screen (Figure 6-7) to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

**Figure 6-7** SNMP Configuration Menu Screen



3583\_15

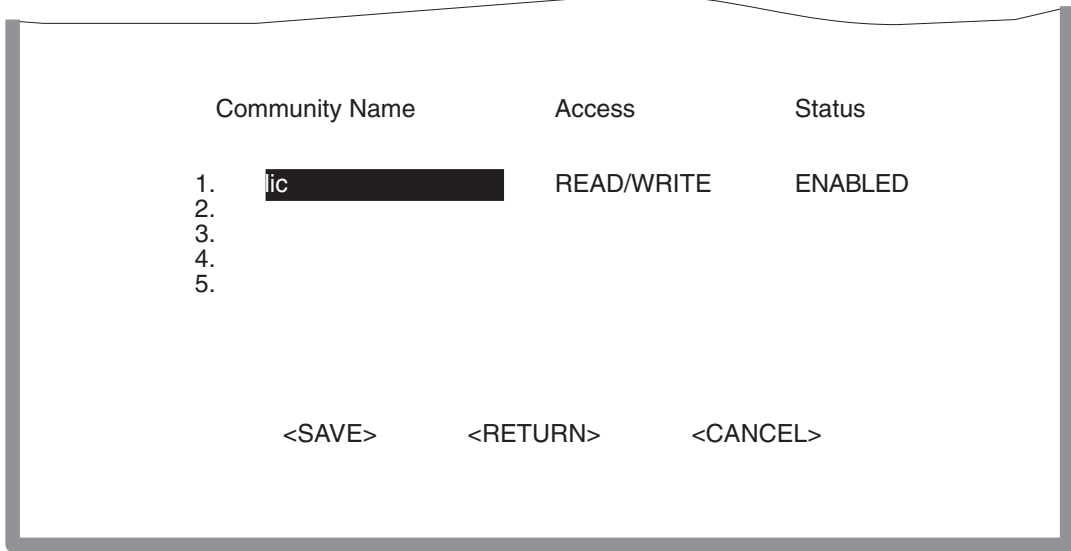
<b>Parameter</b>	<b>Description</b>
Send Authentication Fail Traps	Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default setting is ENABLED.)
SNMP Communities	Provides access to the SNMP Communities screen to assign SNMP access based on specified strings. For details, refer to <a href="#">Section 6.4.1</a> .
IP Trap Managers	Provides access to the IP Trap Managers screen to specify the management stations that will receive authentication failure messages or other trap messages from the switch. For details, refer to <a href="#">Section 6.4.2</a> .

---

### 6.4.1 Configuring Community Names

The SNMP Communities screen (Figure 6-8) is selected from the SNMP Configuration Menu screen. The table following the figure describes the fields. This screen is used to configure the community strings authorized for management access. Up to 5 community names may be entered.

Figure 6-8 SNMP Communities Screen



3583\_16

Parameter	Description
Community Name	A community entry authorized for management access. Maximum string length: 20 characters
Access	Management access is restricted to Read Only or Read/Write.
Status	Sets administrative status of entry to enabled or disabled.



**NOTE:** The default community strings are “public” with Read Only access, and “private” with Read/Write access.

## 6.4.2 Configuring IP Trap Managers

The IP Trap Managers screen (Figure 6-9) is selected from the SNMP Configuration Menu screen. The table following the figure describes the fields. This screen is used to specify the management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

**Figure 6-9 IP Trap Managers Screen**

	IP Address	Community Name	Status
1.	0.0.0.0	public	DISABLED
2.	0.0.0.0	public	DISABLED
3.	0.0.0.0	public	DISABLED
4.	0.0.0.0	public	DISABLED
5.	0.0.0.0	public	DISABLED

<SAVE>                      <RETURN>                      <CANCEL>

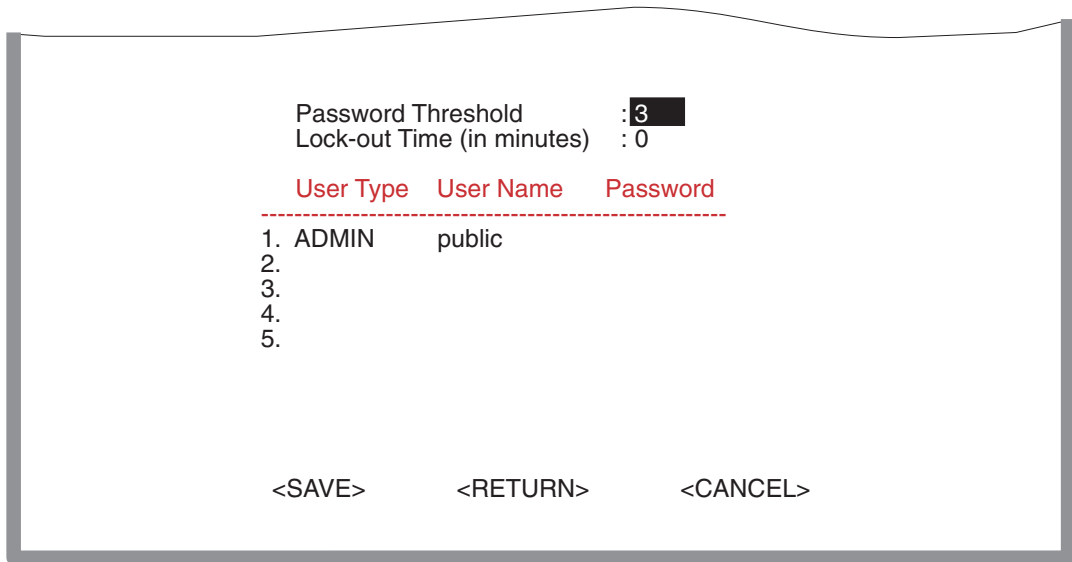
3583\_17

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified for trap management access.
Status	Sets administrative status of selected entry to ENABLED or DISABLED.

## 6.5 CONSOLE LOGIN CONFIGURATION

Use the Console Login Configuration screen (Figure 6-10) to restrict management access based on the specified user names and passwords, or to set the invalid password threshold and time-out. There are two user types: Administrator and Guest. Only the Administrator has write access for parameters governing the SNMP agent. You should therefore assign a user name and password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the System Configuration Program, contact Enterasys Networks for assistance.) The parameters shown on this screen are indicated in the following figure and table.

**Figure 6-10 Console Login Configuration Screen**



3583\_18

Parameter	Default	Description
Password Threshold	3	Sets the password intrusion threshold which limits the number of failed logon attempts. Range: 0-65535
Lock-out Time (in minutes)	0	Sets the time the management console will be disabled, due to an excessive number of failed logon attempts. Range: 0-65535

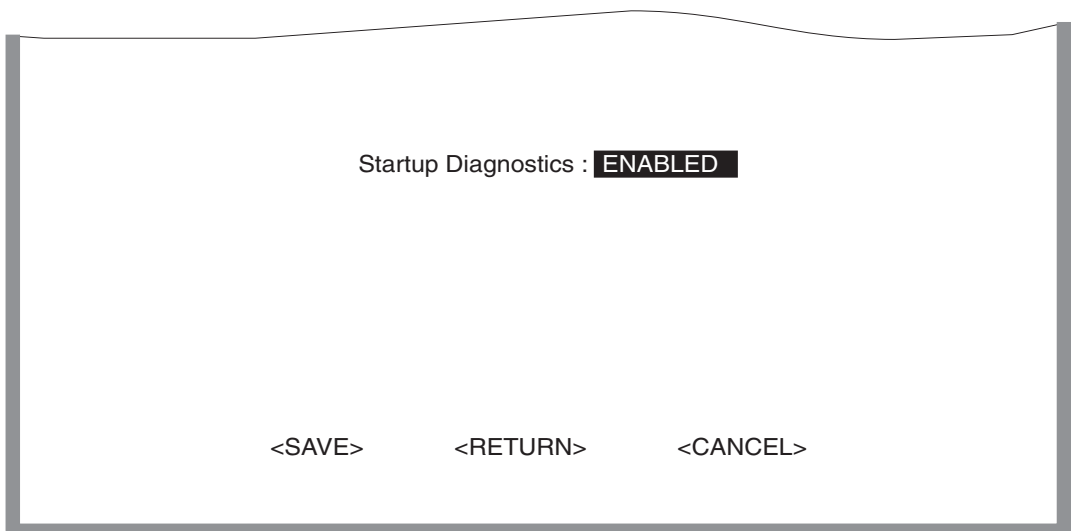


Parameter	Default	Description
User Type	ADMIN	Administrator has access privilege of Read/Write for all screens.
User Name	public	Guest has access privilege of Read Only for all screens.
Password	no password	Passwords can consist of up to 11 alphanumeric characters and are not case sensitive. If there is no password assigned, press ENTER.

## 6.6 SETTING THE STARTUP CONFIGURATION

The Startup Configuration screen (Figure 6-11) is used to disable the extended board diagnostics during the bootup process. When the Startup Diagnostic parameter is set to DISABLED, the diagnostics will not run and the module will bootup in less time. If the module fails and you need to run the diagnostics, change the position of dip switch 5 (on the Mode Switch Bank) on the board and reboot the module. This changes the startup parameter to ENABLED and forces the diagnostics to run when the module is rebooted. For information on the location of the switch and how to set it, refer to the installation guide shipped with your module.

**Figure 6-11 Startup Configuration Screen**



3583\_19

## 6.7 DOWNLOADING SYSTEM SOFTWARE

Use the TFTP Download screen ([Figure 6-12](#)) to perform the following:

- Download a new firmware image file from a TFTP server to the switch module,
- Download a configuration file from a TFTP server to the switch module, or
- Upload the configuration file from the switch module to a TFTP server.

Before downloading an image to the device, copy the image to the network TFTP server. A new firmware image file must be a file from Enterasys Networks; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new image, the agent will automatically restart itself.



**NOTE:** For information on how to set up a workstation as a TFTP server, refer to the specific workstation documentation.

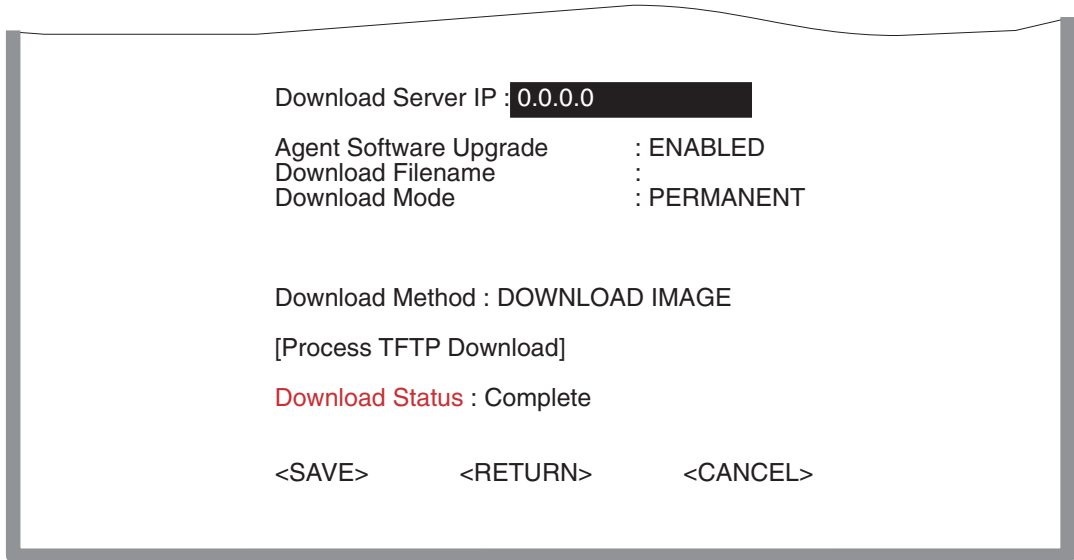
The download and upload configuration capability enables user configured settings to be copied from one switch module to another via the TFTP server, according to the rules described in this section. The configuration file can also be stored on the TFTP server to prevent losing the configuration values while performing maintenance on the switch module. After the maintenance is completed, the configuration values can be downloaded to the same switch module.



**NOTE:** Configuration files cannot be downloaded or uploaded directly from one switch module to another.

The parameters on this screen are shown in [Figure 6-12](#) and described in the following table.

**Figure 6-12 TFTP Download Screen**



3583\_20

Parameter	Description
Download Server IP	IP address of a TFTP server.
Agent Software Upgrade	A community specified for trap management access.
Download Filename	The binary file to download to the agent module.
Download Mode	Downloads to permanent flash ROM.

Parameter	Description
Download Method	<p>Used to select a method (DOWNLOAD IMAGE, UPLOAD CONFIG, or DOWNLOAD CONFIG) to download (receive) an image file from a TFTP server, or upload (transmit) or download a configuration file to/from a TFTP server. The uploading and downloading of a configuration file is accomplished according to the IP address and the file name entered in the Download Server IP and Download File Name fields, respectively.</p> <p>— <b>DOWNLOAD IMAGE</b> – Enables the download of an image from a TFTP server.</p> <p>— <b>UPLOAD CONFIG</b> – Used to upload a configuration file from the switch module to a TFTP server.</p> <p>— <b>DOWNLOAD CONFIG</b> – Used to download a configuration file from a TFTP server to a switch module. The configuration file must be one that was uploaded to the TFTP server from a switch module of the same model with the same optional hardware, and running firmware revision 1.03.xx or higher.</p>
[Process TFTP Download]	Issues a request to the TFTP server to download the specified file.
Download Status	Indicates if a download is “Complete” or “In Progress.”

---

# Device Control Menu Screens

This chapter describes the Device Control Menu screen and the screens that can be selected from its menu to control a broad range of functions.

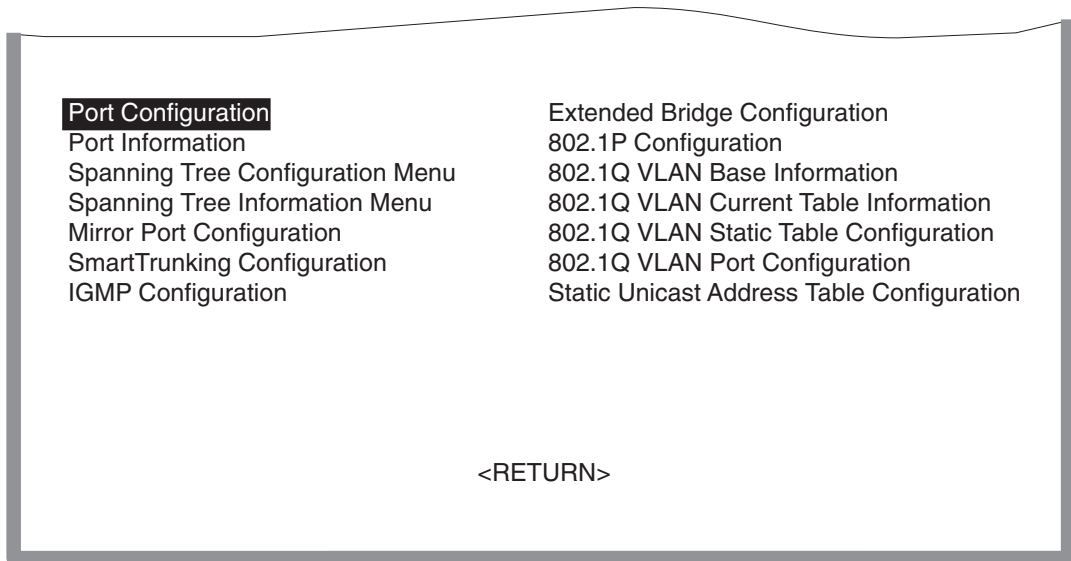
## Screen Navigation Path

Password > Main Menu > **Device Control Menu**

### 7.1 CONFIGURING THE SWITCH

The Device Control Menu screen ([Figure 7-1](#)) is used to control a broad range of functions, including port configuration, Spanning Tree support for redundant switches, port mirroring, multicast filtering, and VLANs. Each of the setup screens provided by these configuration menus is described in the following sections.

Figure 7-1 Device Control Menu Screen



3583\_21

Selection	Description
Port Configuration	Sets communication parameters for ports. For details, refer to <a href="#">Section 7.2</a> .
Port Information	Displays current port settings and port status. For details, refer to <a href="#">Section 7.3</a> .
Spanning Tree Configuration Menu	Configures the switch, its ports and modules to participate in a local Spanning Tree. For details, refer to <a href="#">Section 7.4</a> .
Spanning Tree Information Menu	Displays the current Spanning Tree configuration for the switch, its ports and modules. For details, refer to <a href="#">Section 7.5</a> .
Mirror Port Configuration	Sets the source and target ports for mirroring. For details, refer to <a href="#">Section 7.6</a> .
SmartTrunking Configuration	Specifies ports to group into aggregate trunks. For details, refer to <a href="#">Section 7.7</a> .

---

Selection	Description
IGMP Configuration	Configures IGMP multicast filtering. For details, refer to <a href="#">Section 7.8</a> .
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, and VLAN extensions. For details, refer to <a href="#">Section 7.9</a> .
802.1P Configuration	Used to configure the default port priorities and queue assignments for each port, or to display the mapping for the traffic classes. For details, refer to <a href="#">Section 7.10</a> .
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported. For details, refer to <a href="#">Section 7.11</a> and <a href="#">Section 7.12</a> .
802.1Q VLAN Current Table Information	Displays VLAN groups and port members. For details, refer to <a href="#">Section 7.13</a> .
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members. For details, refer to <a href="#">Section 7.14</a> .
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, and ingress filtering. For details, refer to <a href="#">Section 7.15</a> .
Static Unicast Address Table Configuration	Allows you to display or configure static unicast addresses. For details, refer to <a href="#">Section 7.16</a> .

---

## 7.2 CONFIGURING PORT PARAMETERS

Use the Port Configuration screen (Figure 7-2) to set or display communication parameters for any port or module on the switch.

Figure 7-2 Port Configuration Screen

Port Configuration : Port 1 - 12

Flow Control mode of all ports : **[Enable]** [Disable]

Port	Type	Admin	Flow Control	Speed and Duplex
1	10/100TX	ENABLED	ENABLED	AUTO
2	10/100TX	ENABLED	ENABLED	AUTO
3	10/100TX	ENABLED	ENABLED	AUTO
4	10/100TX	ENABLED	ENABLED	AUTO
5	10/100TX	ENABLED	ENABLED	AUTO
6	10/100TX	ENABLED	ENABLED	AUTO
7	10/100TX	ENABLED	ENABLED	AUTO
8	10/100TX	ENABLED	ENABLED	AUTO
9	10/100TX	ENABLED	ENABLED	AUTO
10	10/100TX	ENABLED	ENABLED	AUTO
11	10/100TX	ENABLED	ENABLED	AUTO
12	10/100TX	ENABLED	ENABLED	AUTO

<SAVE> <RETURN> <CANCEL> <PREV PAGE> <NEXT PAGE>

3583\_22



---

Parameter	Default	Description
Type		Shows port type as: 10/100TX: 10Base-T/100Base-TX 100FX: 100Base-FX 1000SX: 1000Base-SX 1000LX: 1000Base-LX
Admin	ENABLED	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Flow Control	DISABLED	Used to enable or disable flow control. Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Do not use flow control if a port is connected to a hub.
Speed and Duplex	AUTO	Used to set the current port speed, duplex mode, and auto-negotiation. (Auto-negotiation is not available for 100Base-FX ports.)

---

### 7.3 VIEWING THE CURRENT PORT CONFIGURATION

The Port Information screen (Figure 7-3) displays the port type, status, link state, and flow control in use, as well as the communication speed and duplex mode. To change any of the port settings, use the Port Configuration menu. The parameters shown in the following figure and table are for the RJ45 ports.

Figure 7-3 Port Information Screen

Port Information : Port 1 - 12						
Port	Type	Operational	Link	FlowControl InUse	Speed and Duplex InUse	
1	10/100TX	YES	UP	Back_Pressure	10_HALF	
2	10/100TX	YES	DOWN	-----	-----	
3	10/100TX	YES	DOWN	-----	-----	
4	10/100TX	YES	DOWN	-----	-----	
5	10/100TX	YES	DOWN	-----	-----	
6	10/100TX	YES	DOWN	-----	-----	
7	10/100TX	YES	DOWN	-----	-----	
8	10/100TX	YES	DOWN	-----	-----	
9	10/100TX	YES	DOWN	-----	-----	
10	10/100TX	YES	DOWN	-----	-----	
11	10/100TX	YES	DOWN	-----	-----	
12	10/100TX	YES	DOWN	-----	-----	

<RETURN>
<PREV PAGE>
<NEXT PAGE>

3583\_23

---

<b>Parameter</b>	<b>Description</b>
Type	Shows port type as: 10/100TX: 10Base-T/100Base-TX 100FX: 100Base-FX 1000SX: 1000Base-SX 1000LX: 1000Base-LX
Operational	Shows if the port is, or is not, functioning.
Link	Indicates if the port has a valid connection to an external device.
Flow Control InUse	Shows the flow control type in use. Flow control can eliminate frame loss by “blocking” traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Speed and Duplex InUse	Displays the current port speed and duplex mode used.

---

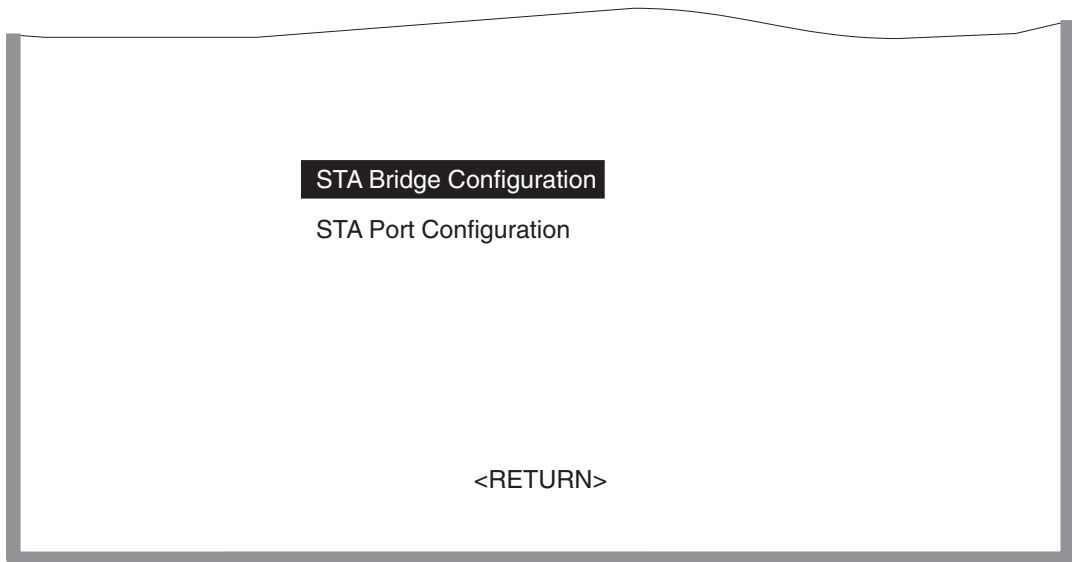
## 7.4 USING THE SPANNING TREE ALGORITHM

The Spanning Tree Algorithm (STA) is used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. The Spanning Tree Configuration:Selection Menu screen (Figure 7-4) provides a menu selection to gain access to the STA Bridge Configuration and STA Port Configuration screens to configure the STA functions.

To view the current STA bridge and port information, refer to [Section 7.5](#).

For a more detailed description of how to use this algorithm, refer to [Appendix A](#).

**Figure 7-4 Spanning Tree Configuration:Selection Menu Screen**



3583\_24

## 7.4.1 Configuring STA Bridge

The STA Bridge Configuration screen (Figure 7-5) to set the STA Bridge parameters. The following table describes the STA Bridge configuration parameters.

**Figure 7-5 STA Bridge Configuration Screen**

```

Spanning Tree Protocol      : ENABLED
Priority                    : 32768
Hello Time (in seconds)    : 2
Max Age (in seconds)       : 20
Forward Delay (in seconds) : 15

<SAVE>      <RETURN>      <CANCEL>
  
```

3583\_25

Parameter	Default	Description
Spanning Tree Protocol	ENABLED	Enables this parameter to participate in an STA compliant network.
Priority	32768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.  Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.

Parameter	Default	Description
Hello Time (in seconds)	2	<p>Time interval at which the root device transmits a configuration message.</p> <p>The minimum value is 1. The maximum value is the lower of 10 or <math>[(\text{Max. Message Age} / 2) - 1]</math>.</p>
Max Age (in seconds)	20	<p>The maximum time a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.</p> <p>The minimum value is the higher of 6 or <math>[2 \times (\text{Hello Time} + 1)]</math>. The maximum value is the lower of 40 or <math>[2 \times (\text{Forward Delay} - 1)]</math>.</p>
Forward Delay (in seconds)	15	<p>The maximum time the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.</p> <p>The maximum value is 30. The minimum value is the higher of 4 or <math>[(\text{Max. Message Age} / 2) + 1]</math>.</p>

## 7.4.2 Configuring STA for Ports

Use the STA Port Configuration screen (Figure 7-6) to set the STA port parameters. The following table describe the STA configuration parameters for the ports.

**Figure 7-6 STA Tree Port Configuration Screen**

Spanning Tree Port Configuration :Port 1 - 12

Fast forwarding mode of all ports : **[Enable]** [Disable]

Port	Type	Priority	Cost	FastForwarding
1	10/100TX	128	100	ENABLED
2	10/100TX	128	10	ENABLED
3	10/100TX	128	10	ENABLED
4	10/100TX	128	10	ENABLED
5	10/100TX	128	10	ENABLED
6	10/100TX	128	10	ENABLED
7	10/100TX	128	10	ENABLED
8	10/100TX	128	10	ENABLED
9	10/100TX	128	10	ENABLED
10	10/100TX	128	10	ENABLED
11	10/100TX	128	10	ENABLED
12	10/100TX	128	10	ENABLED

<SAVE> <RETURN> <CANCEL> <PREV PAGE> <NEXT PAGE>

3583\_26

Parameter	Default	Description
Type		Shows 10/100TX, 100FX, 1000LX or 1000SX port.
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.  The range is 0 - 255.

Parameter	Default	Description
Cost	100/19/4	<p>This parameter (path cost) is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.</p> <p>(Path cost takes precedence over port priority.)</p> <p>The default and recommended range is:</p> <p>Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535.</p>
Fast Forwarding	ENABLED	<p>Enables or disables the port to forward packets. All ports currently displayed can be enabled or disabled at once using the command near the top of the screen.</p>

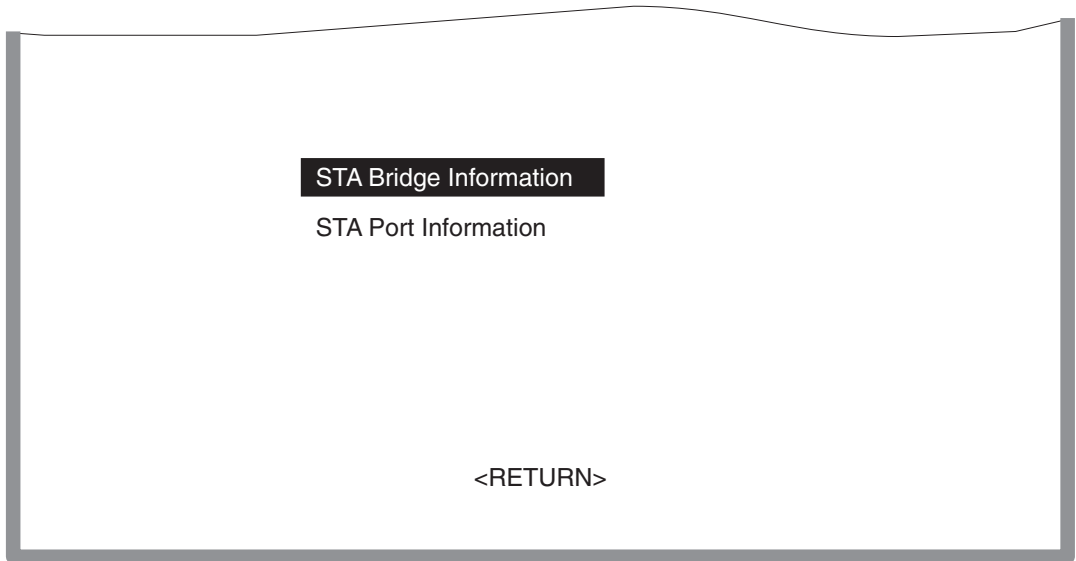
---



## 7.5 VIEWING THE CURRENT SPANNING TREE CONFIGURATION

The Spanning Tree Information: Selection Menu screen (Figure 7-7) enables you to select one of two screens to display a summary of the STA information for the overall bridge or for a specific port. To make changes to the STA bridge or STA port operating parameters, refer back to Section 7.4.

**Figure 7-7 Spanning Tree Information: Selection Menu Screen**

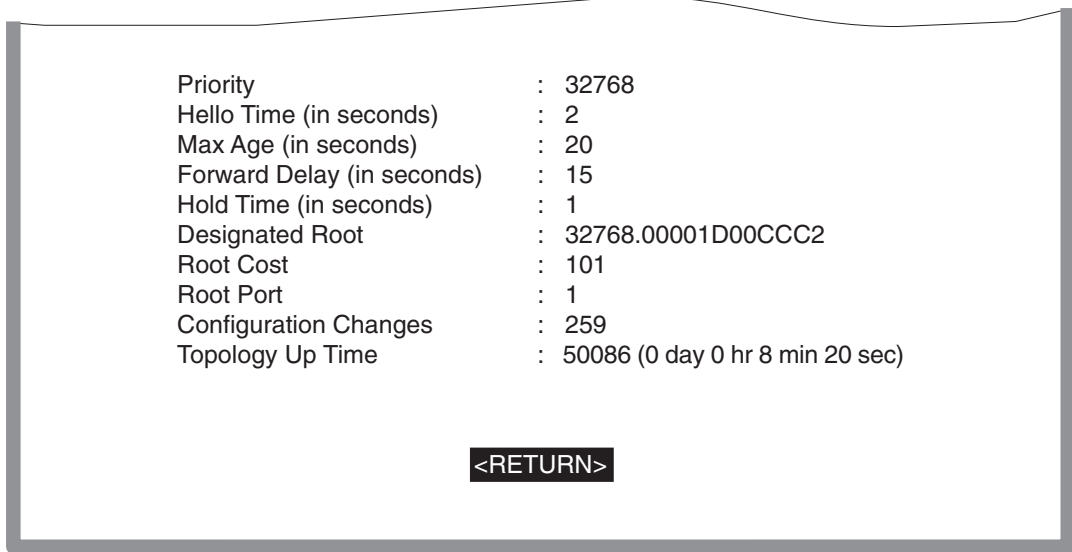


3583\_27

## 7.5.1 Displaying the Current STA Bridge

The STA Bridge Information screen (Figure 7-8) displays the current information about the STA Bridge. The following table describes the parameters shown on the screen.

**Figure 7-8 STA Bridge Information Screen**



3583\_28

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time (in seconds)	The time interval at which the root device transmits a configuration message.
Max Age (in seconds)	The maximum time a device can wait without receiving a configuration message before attempting to reconfigure.

<b>Parameter</b>	<b>Description</b>
Forward Delay (in seconds)	The maximum time the root device will wait before changing states (i.e., from listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Configuration Changes	The number of times the spanning tree has been reconfigured.
Topology Up Time	The time since the spanning tree was last reconfigured.

## 7.5.2 Displaying the Current STA for Ports or Modules

The parameters shown in the following STA Port Information screen (Figure 7-4) and table are for port STA Information (Ports 1-12, Ports 13-24, Ports 25-36, or Ports 37-48).



**NOTE:** The actual number of ports varies depending on the module.

Figure 7-9 STA Port Information Screen

Spanning Tree Port Information : Port 1 - 12					
Port	Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	FORWARDING	9	1	32768.00001D64A189	128.22
2	FORWARDING	1	101	32768.0000E8000500	128.2
3	FORWARDING	1	101	32768.0000E8000500	128.3
4	FORWARDING	1	101	32768.0000E8000500	128.4
5	FORWARDING	1	101	32768.0000E8000500	128.5
6	FORWARDING	1	101	32768.0000E8000500	128.6
7	FORWARDING	1	101	32768.0000E8000500	128.7
8	FORWARDING	1	101	32768.0000E8000500	128.8
9	FORWARDING	1	101	32768.0000E8000500	128.10
11	FORWARDING	1	101	32768.0000E8000500	128.11
12	FORWARDING	1	101	32768.0000E8000500	128.12

3583\_29

---

Parameter	Description
Status	<p data-bbox="552 239 1228 300">Displays the current state of this port within the spanning tree:</p> <p data-bbox="552 326 1237 387">Disabled – Port has been disabled by the user or has failed diagnostics.</p> <p data-bbox="552 413 1237 473">Blocking – Port receives STA configuration messages, but does not forward packets.</p> <p data-bbox="552 499 1251 604">Listening – Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets.</p> <p data-bbox="552 630 1233 760">Learning – Has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.</p> <p data-bbox="552 786 1204 847">Forwarding – The port forwards packets, and continues learning addresses.</p> <p data-bbox="552 873 946 899">The rules defining port status are:</p> <ul data-bbox="552 925 1251 1263" style="list-style-type: none"><li data-bbox="552 925 1157 986">• A port on a network segment with no other STA compliant bridging device is always forwarding.</li><li data-bbox="552 1012 1251 1142">• If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked.</li><li data-bbox="552 1168 1237 1263">• All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.</li></ul>
Forward Transitions	Number of frames forwarded out the port.
Designated Cost	The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.

---

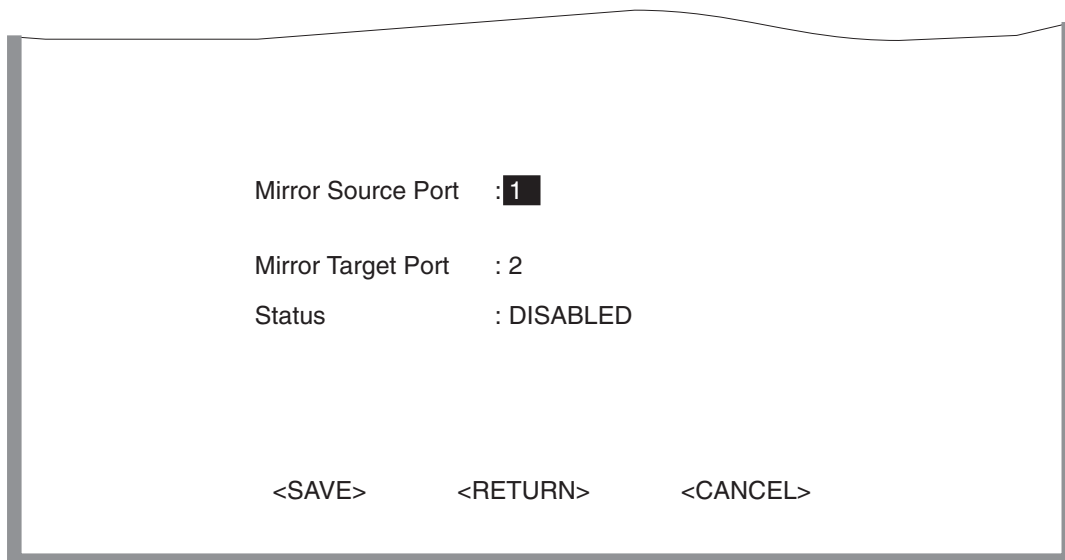
Parameter	Description
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
Designated Port (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

## 7.6 USING A MIRROR PORT FOR ANALYSIS

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be configured in the same VLAN and be operating at the same speed as the source port. (Refer to [Section 7.11](#) for information on configuring virtual VLANs.) If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

Use the Mirror Port Configuration screen ([Figure 7-10](#)) to designate a single port pair (source and target ports) for mirroring.

**Figure 7-10** Mirror Port Configuration Screen



3583\_30

Parameter	Description
Mirror Source Port	The port on which traffic will be monitored.
Mirror Target Port	The port that will duplicate or “mirror” all the traffic on the monitored port.
Status	Enables or disables the mirror function.

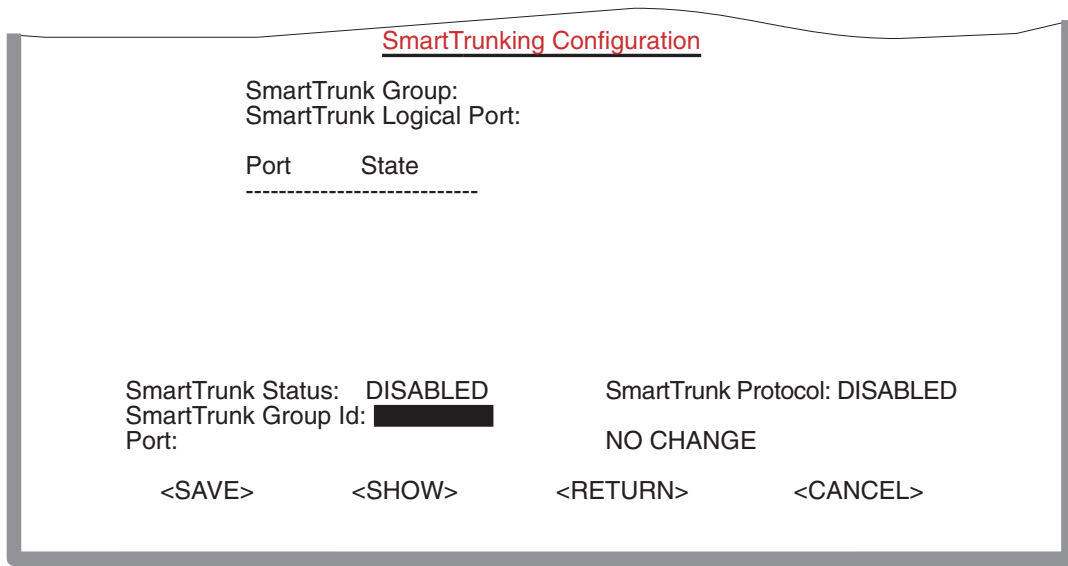
## 7.7 CONFIGURING SMARTTRUNKS

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up six trunk connections (combining 2 through 8 ports into a fat pipe) between any two switches. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- The trunk ports must all be front panel ports.
- Ports can only be assigned to one trunk.
- The ports in a trunk must belong to the same switch chip (refer to [Table 7-1](#)).
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.
- The communication mode must be configured identically at both ends of the trunk.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- You must enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- You must disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

Use the Smart Trunking Configuration screen (Figure 7-11) to set up port trunks.

**Figure 7-11 SmartTrunking Configuration Screen**



3583\_31

Parameter	Description
SmartTrunk Group	Read only field that indicates the SmartTrunk Group number associated with the logical ports listed under SmartTrunk Logical Port.
SmartTrunk Logical Port	Read only field that lists the Logical Ports associated with the SmartTrunk Group
SmartTrunk Status	Used to enable or disable the trunk group
SmartTrunk Group ID	Used to select from 1 to 6 trunks. This is the group ID of the SmartTrunk group. Identifies the chip set to be used. Refer to Table 7-1 for the ports associated with each group ID.
Port	Lists the valid ports for the chip set selected in the SmartTrunk Group ID field. Refer to Table 7-1 for the ports associated with each group ID.



Parameter	Description
SmartTrunk Protocol	Used to select from 1 to 6 trunks. This is the group ID of the SmartTrunk group. It identifies the chip set to be used. Refer to <a href="#">Table 7-1</a> for the ports associated with each group ID.
NO CHANGE field	Used to add or delete ports from group ID. Steps to ADD, DELETE, and NO CHANGE (default setting). This setting causes the port selected in the Port field to be added, deleted, or not changed when SAVE command is used.
SAVE	Saves the current values on the screen.
SHOW	Displays the SmartTrunk group listed under the SmartTrunk Group ID field.

The ports used for each trunk must all be on the same internal switch chip, which is synonymous with the SmartTrunk Group ID. [Table 7-1](#) identifies the ports associated with each group ID.

**Table 7-1 SmartTrunk, Ports Associated with Group IDs**

Group IDs	1	2	3	4	5	6
Ports	1 thru 8	9 thru 16	17 thru 24	25 thru 32	33 thru 40	41 thru 48

## 7.7.1 IGMP Multicast Filtering

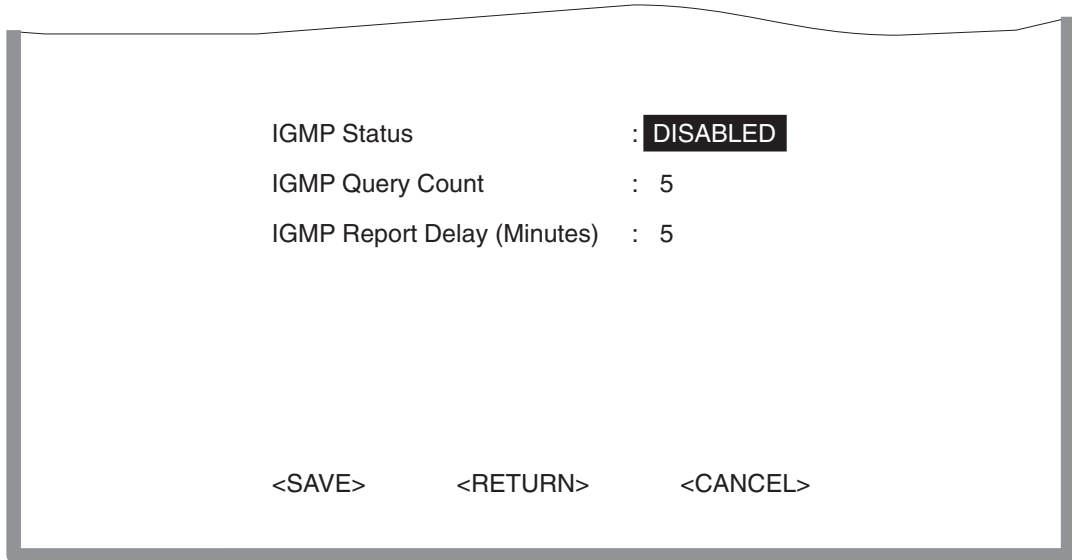
Multicasting is used to support real-time applications such as video conferences or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed to the hosts that subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port that received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information about the use of IGMP snooping and multicast filtering, refer to [Appendix D](#).)

## 7.8 CONFIGURING IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast group. Use the IGMP Configuration screen (Figure 7-12) to configure multicast filtering.

**Figure 7-12 IGMP Configuration Screen**



3583\_32



**NOTE:** The default values are shown in [Figure 7-12](#).

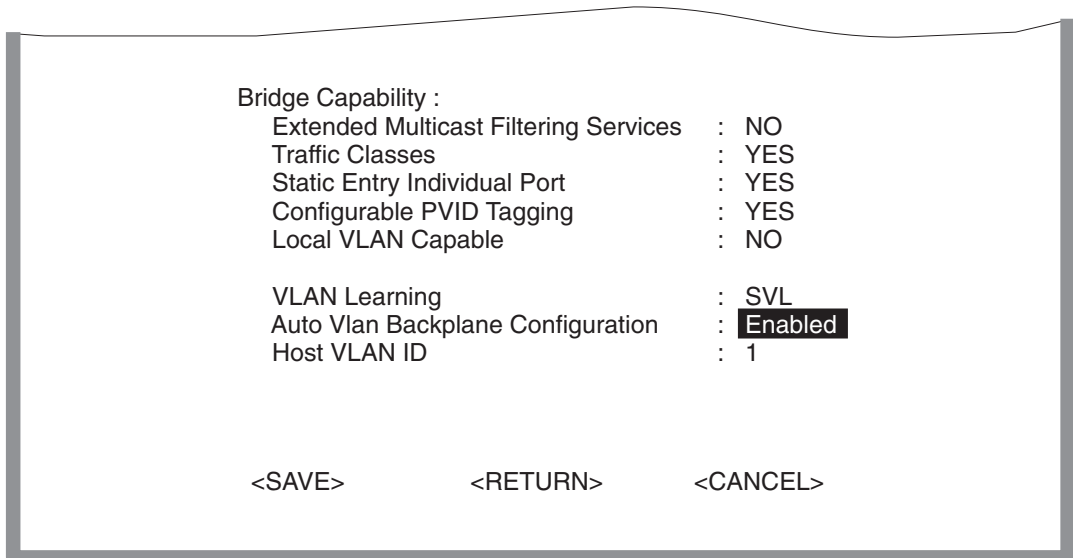
Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

Parameter	Description
IGMP Query Count	The time in minutes that must elapse before the switch removes the port from an IGMP group. This timer is started after the number of queries are missed as defined in the IGMP Query Count.
IGMP Report Delay (Minutes)	The number of queries that must be missed before the IGMP Report Delay timer is started. This is used in conjunction with the IGMP Report Delay to remove ports from an IGMP group.


## 7.9 CONFIGURING BRIDGE MIB EXTENSIONS

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and VLANs. To see the current settings for these extensions, select and enable or disable a VLAN Learning mode, use the Extended Bridge Configuration screen (Figure 7-13).

**Figure 7-13 Extended Bridge Configuration Screen**



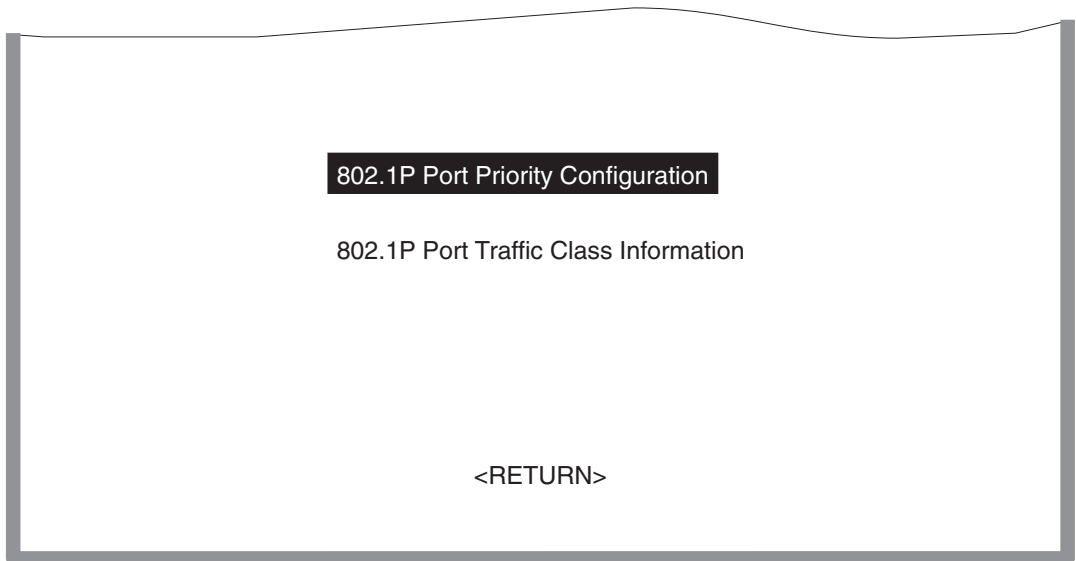
3583\_33

Parameter	Description
Extended Multicast Filtering Services	<p>Indicates if the filtering of individual multicast addresses based on Multicast Registration Protocol is active.</p> <p> <b>NOTE:</b> This function is not available for the current firmware release.</p>
Traffic Classes	Indicates if the mapping of user priorities to multiple traffic classes function is active. (For configuration information, refer to <a href="#">Section 7.10.</a> )
Static Entry Individual Port	Indicates if the static filtering for unicast and multicast addresses function is active. (For configuration information, refer to <a href="#">Section 7.16.</a> )
Configurable PVID Tagging	Allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. For details, refer to <a href="#">Section 7.15.</a>
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).
VLAN Learning	<p>Allows you to select the VLAN Learning mode (IVL or SVL) used by the switch.</p> <p><b>IVL</b> (Independent VLAN Mode) – Allows addresses to be learned per VLAN.</p> <p><b>SVL</b> (Shared VLAN Mode) – Allows a single address for all VLANs.</p>
Auto VLAN Backplane Configuration	<p>Enables or disables the ports on the backplane to support automatic configuration of VLANs. The default is Enabled.</p> <p>When set to Disabled, you must configure VLANs manually. For information on how to configure VLANs manually, refer to <a href="#">Section 7.15.</a></p>
Host VLAN ID	Allows you to enter the Host VLAN ID and it is not limited to the default VLAN (1).

## 7.10 CONFIGURING TRAFFIC CLASSES

IEEE 802.1p defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with weighted fair queuing for each port. You can use the 802.1P Configuration Menu screen (Figure 7-14) to access the screens to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections. Also, refer to [Appendix C](#), for information on Class of Service.

**Figure 7-14 802.1P Configuration Menu Screen**

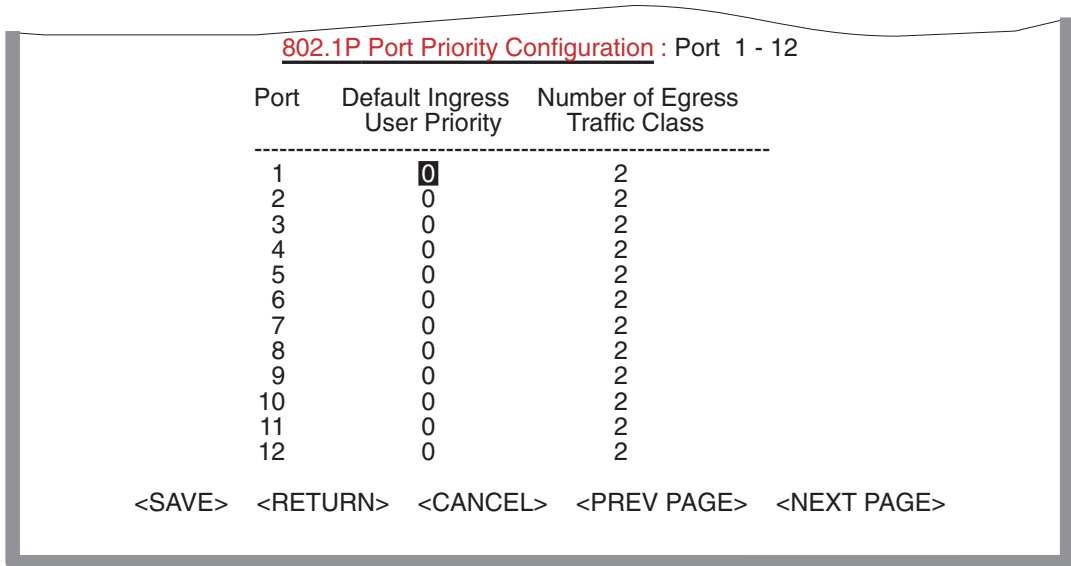


3583\_34

### 7.10.1 Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the 802.1P Port Priority Configuration menu screen (Figure 7-15) to adjust the default priority for any port.

**Figure 7-15 802.1P Port Priority Configuration Screen**



3583\_35

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0~7, where 0~3 specifies the low priority queue and 4~7 specifies the high priority queue.
Number of Egress Traffic Class	Indicates that this switch supports two priority output queues.

### 7.10.2 802.1P Port Traffic Class Information

This switch provides two priority levels with weighted fair queuing for port egress. This means that any frames with a default or user priority from 0~3 are sent to the low priority queue “0” while those from 4~7 are sent to the high priority queue “1” as shown in [Figure 7-16](#).

Figure 7-16 802.1P Port Traffic Class Information Screen

**802.1P Port Traffic Class Information** : Port 1 - 12

Port	User Priority							
	0	1	2	3	4	5	6	7
1	0	0	0	0	1	1	1	1
2	0	0	0	0	1	1	1	1
3	0	0	0	0	1	1	1	1
4	0	0	0	0	1	1	1	1
5	0	0	0	0	1	1	1	1
6	0	0	0	0	1	1	1	1
7	0	0	0	0	1	1	1	1
8	0	0	0	0	1	1	1	1
9	0	0	0	0	1	1	1	1
10	0	0	0	0	1	1	1	1
11	0	0	0	0	1	1	1	1
12	0	0	0	0	1	1	1	1

<RETURN>
<PREV PAGE>
<NEXT PAGE>

3583\_36

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0~3 specify the low priority queue and 4~7 specify the high priority queue.

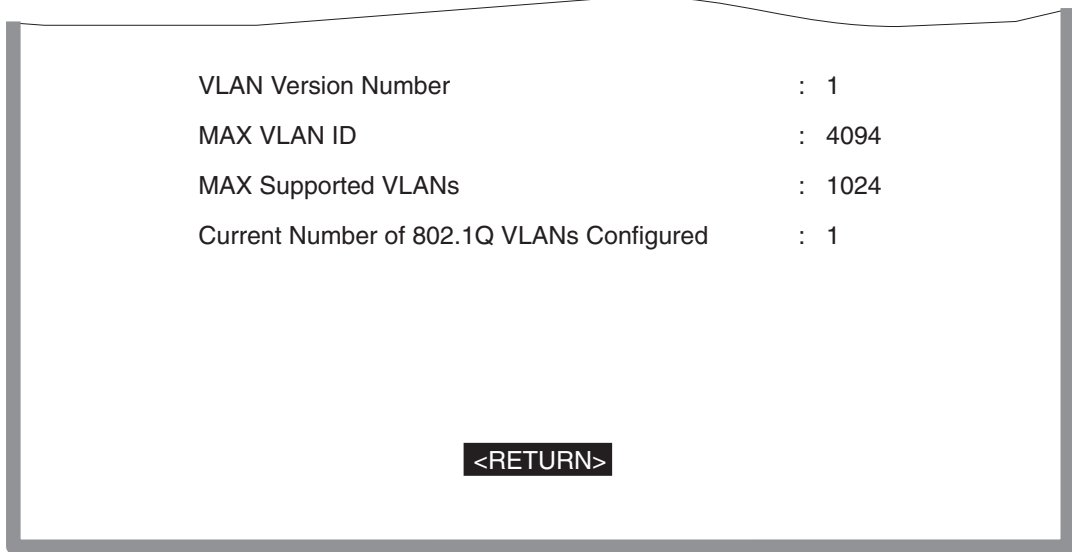
## 7.11 CONFIGURING VIRTUAL LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 1024 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of IPX traffic. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, refer to [Appendix B](#). The VLAN configuration screens are described in the following sections.

## 7.12 802.1Q VLAN BASE INFORMATION

The 802.1Q VLAN Base Information screen (Figure 7-17) displays basic information on the VLAN type supported by this switch.

**Figure 7-17 802.1Q VLAN Base Information Screen**



3583\_37

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of 802.1Q VLANs Configured	The number of VLANs currently configured on this switch.



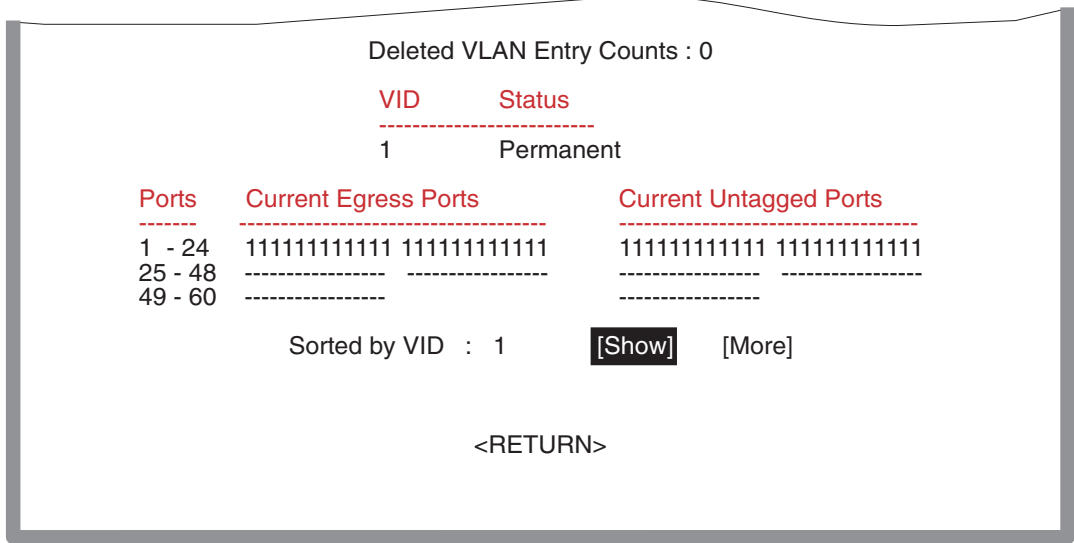
### 7.13 802.1Q VLAN CURRENT TABLE INFORMATION

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN (refer to [Section 7.15](#)). The current configuration is shown in [Figure 7-18](#).



**NOTE:** Under the screen field heading of Egress Ports, Forbidden Egress Ports, or Tagged Ports, each number (1 or 0) represents a port. For example, next to 1 - 24 under the Ports field heading, the leftmost number represents the port 1 and the rightmost number represents port 24.

**Figure 7-18 802.1Q VLAN Current Table Information Screen**



3583\_38

Parameter	Description
Deleted VLAN Entry Counts	The number of times a VLAN entry has been deleted from this table.
VID	The ID for the VLAN currently displayed.

Parameter	Description
Status	Shows how this VLAN was added to the switch.
Current Egress Ports	Shows the ports which have been added to the displayed VLAN group, where “1” indicates that a port is a member and “0” that it is not.
Current Untagged Ports	If a port has been added to the displayed VLAN (shown Current Egress Ports field), its entry in this field will be “1” if the port is untagged or “0” if tagged.
[Show]	Displays the members for the VLAN indicated by the “Sorted by VID” field.
[More]	Displays any subsequent VLANs if configured.

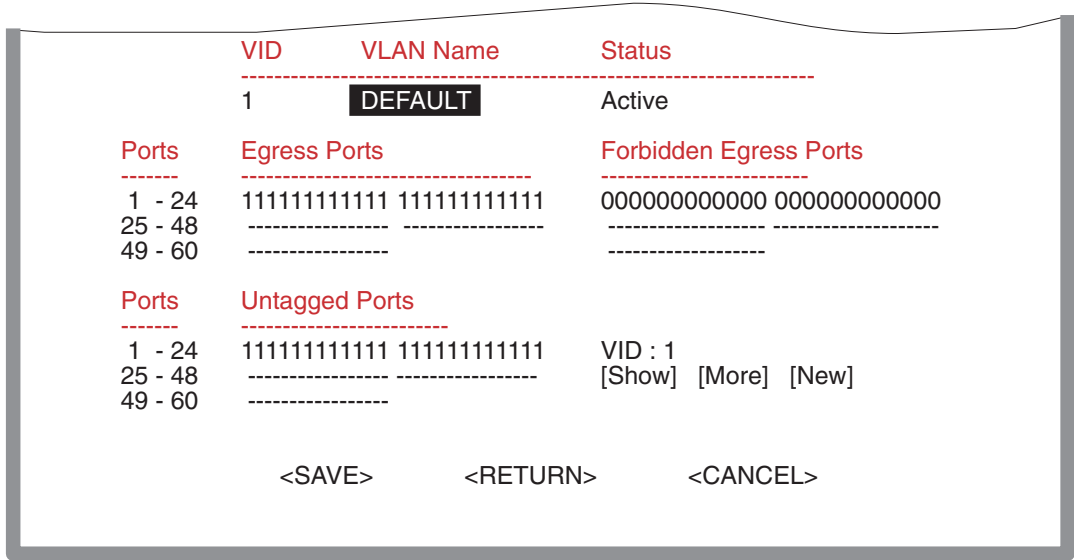
## 7.14 802.1Q VLAN STATIC TABLE CONFIGURATION

Use the 802.1Q VLAN Static Table Configuration screen ([Figure 7-19](#)) to create a new VLAN or modify the settings for an existing VLAN. You can add/delete port members of any VLAN in the switch. (Also, note that all ports can only belong to one untagged VLAN. This is set to VLAN 1 by default, but can be changed via the 802.1Q VLAN Port Configuration screen described in [Section 7.15](#).)



**NOTE:** Under the screen field heading of Egress Ports, Forbidden Egress Ports, or Tagged Ports, each number (1 or 0) represents a port. For example, next to 1 - 24 under the Ports field heading, the leftmost number represents the port 1 and the rightmost number represents port 24.

Figure 7-19 802.1Q VLAN Static Table Configuration Screen



3583\_39

Parameter	Description
VID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
Status	Sets the current editing status for this VLAN as: Not in Service, Destroy, or Active.
Egress Ports	Sets one or more port entries in this field to “1” to add, or “0” to remove it from the VLAN displayed on the screen.
Forbidden Egress Ports	Sets one or more port entries in this field to “1” to prevent from being added to this VLAN.
Untagged Ports	Sets the entry for any port in this field to “1” to enable the recognition of untagged frames to this VLAN.

Parameter	Description
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANs.
[New]	Sets up the screen for configuring a new VLAN.

## 7.15 802.1Q VLAN PORT CONFIGURATION

Use the 802.1Q VLAN Port Configuration screen (Figure 7-20) to configure port-specific settings for IEEE 802.1Q VLAN features.

Figure 7-20 802.1Q VLAN Port Configuration Screen

802.1Q VLAN Port Configuration : Port 1 - 12

Port	PVID	Acceptable Frame Type	Ingress Filtering
1	<b>1</b>	ALL	FALSE
2	1	ALL	FALSE
3	1	ALL	FALSE
4	1	ALL	FALSE
5	1	ALL	FALSE
6	1	ALL	FALSE
7	1	ALL	FALSE
8	1	ALL	FALSE
9	1	ALL	FALSE
10	1	ALL	FALSE
11	1	ALL	FALSE
12	1	ALL	FALSE

<SAVE>   <RETURN>   <CANCEL>   <PREV PAGE>   <NEXT PAGE>

3583\_40

---

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type*	This switch accepts “All” frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering*	If set to “True,” incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.

---

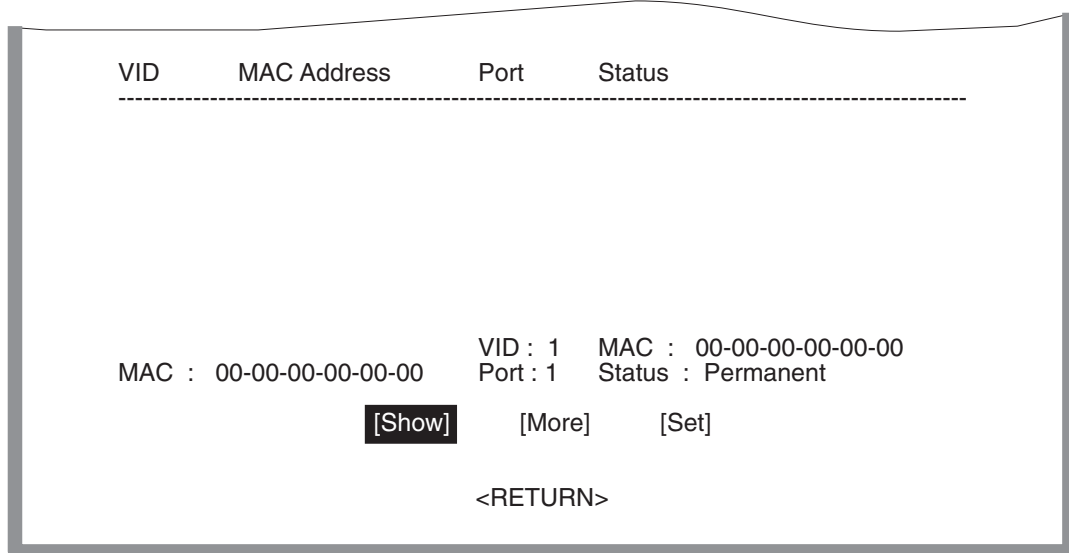
\* This control does not affect VLAN independent BPDU frames, such as STP.

## 7.16 CONFIGURING STATIC UNICAST ADDRESSES

Use the Static Unicast Address Table Configuration screen (Figure 7-21) to manually configure host MAC addresses in the unicast table. You can use this screen to associate a MAC address with a specific VLAN ID and switch port.

You can also lock a port to a particular MAC Address or the first MAC address received by the port to prevent other users (MAC Addresses) from using that port. When a port is locked, broadcast and multicast packets are processed over the link as well as the locked MAC address packets.

**Figure 7-21 Static Unicast Address Table Configuration Screen**



3583\_41

Parameter	Description
VID	The VLAN group to which this port is assigned.
MAC Address	The MAC address of a host device attached to this switch.
Port	The port to which the host device is attached.

Parameter	Description
Status	<p>The status for an entry can be set to:</p> <p>Permanent—This entry is currently in use and will remain so after the next reset of the switch.</p> <p>DeleteOnReset—This entry is currently in use and will remain so until the next reset.</p> <p>Lock Port—Enables the port locking mode. For details, refer to <a href="#">Section 10.15.1</a>.</p> <p>Unlock Port—Disables the port locking mode. For details, refer to <a href="#">Section 10.15.2</a>.</p> <p>Invalid—Removes the corresponding entry.</p> <p>DeleteOnTimeOut—This entry is currently in use and will remain so until it is aged out. (Refer to Aging Time in <a href="#">Section 8.4</a>.)</p> <p>Other—This entry is currently in use, but the conditions under which it will remain, differ from the preceding values.</p>
[Show]	Displays the static address table sorted on VID as the primary key and MAC address as secondary key.
[More]	Scrolls through entries in the static address table.
[Set]	<p>Adds the specified entry to the static address table, such as shown in the following example:</p> <p style="padding-left: 40px;">VID: 1 MAC: 00-00-00-e8-34-22 Unit: 1 Port: 1 Status: Permanent</p>





---

# Network Monitoring Menu Screens

This chapter describes the Network Monitor Menu screen and the screens that can be selected from its menu.

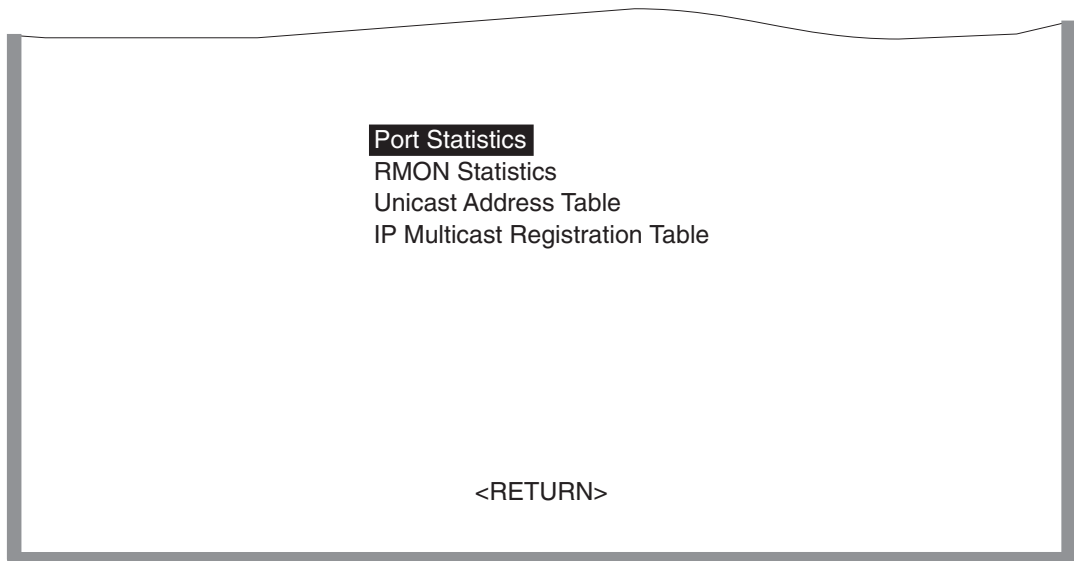
## Screen Navigation Path

Password > Main Menu > **Network Monitor Menu**

### 8.1 MONITORING THE SWITCH

The Network Monitor Menu screen (Figure 8-1) provides access to port statistics, RMON statistics, IP multicast addresses, and the static (unicast) address table. Each of the screens provided by these menus is described in the following sections.

**Figure 8-1 Network Monitor Menu Screen**



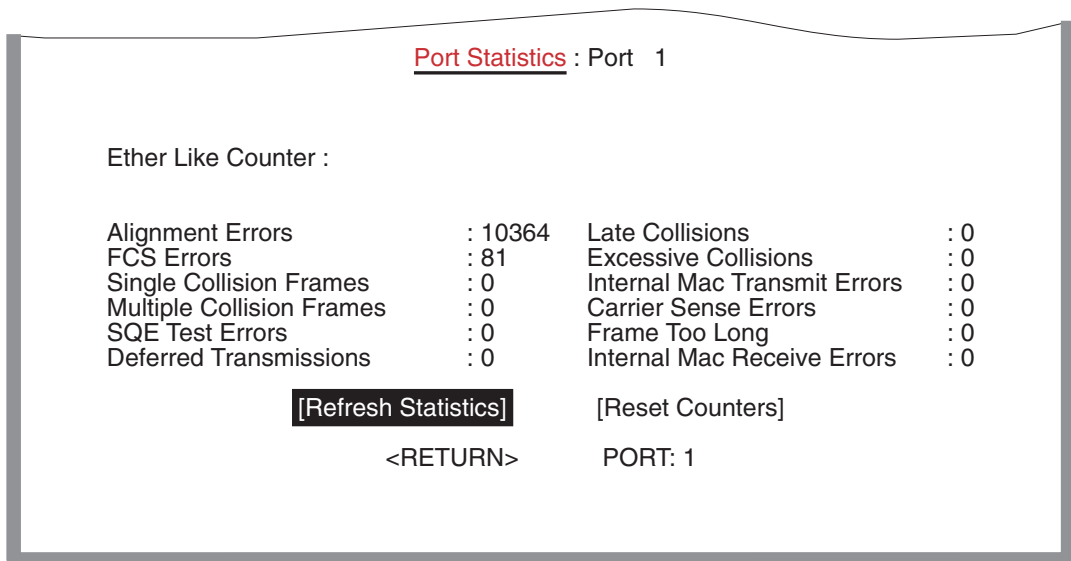
3583\_42

Parameter	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing of all unicast addresses stored in the switch, as well as sort, search and clear functions.
IP Multicast Registration Table	Displays the ports that belong to each IP Multicast group.

## 8.2 DISPLAYING PORT STATISTICS

The Port Statistics screen (Figure 8-2) displays the key statistics from the Ethernet-like MIB for each port. Error statistics on the traffic passing through each port are also displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). The values displayed have been accumulated since the last system reboot. Select the required port or module. The statistics displayed are indicated in Figure 8-2 and described in the following table.

**Figure 8-2 Port Statistics Screen**



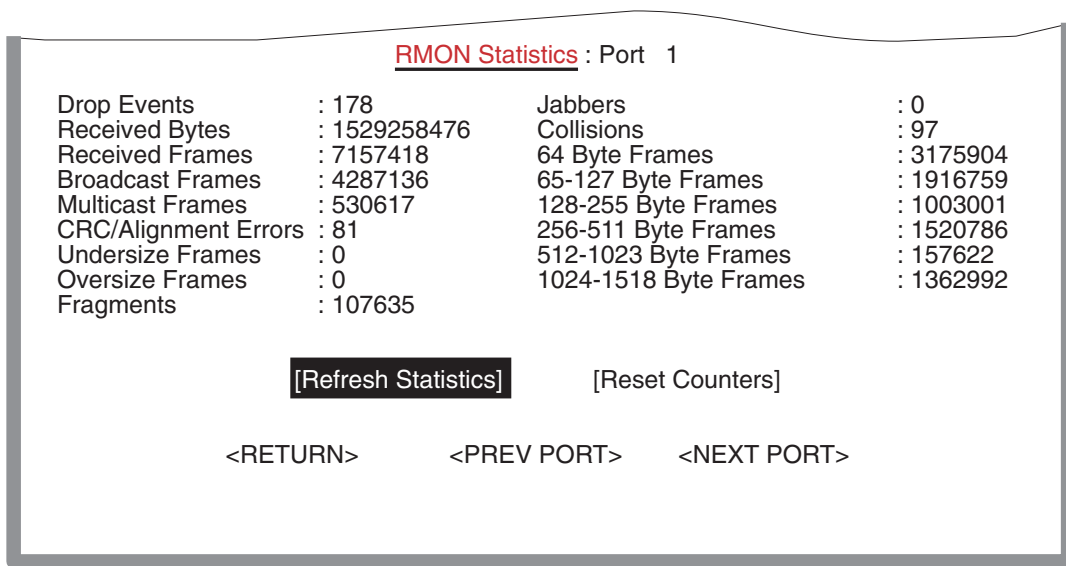
Parameter	Description
Alignment Errors	For 10 Mbps ports, this counter records alignment errors (mis-synchronized data packets). For 100 Mbps ports, this counter records the sum of alignment errors and code errors (frames received with rxerror signal).
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors*	The number of frames for which reception failed due to an internal MAC sublayer receive error.

\* The reported values will always be zero because these statistics are not supported by the internal chip set.

### 8.3 DISPLAYING RMON STATISTICS

Use the RMON Statistics screen (Figure 8-3) to display key statistics for each port or media module from RMON group 1. (RMON groups 2, 3 and 4 can only be accessed using SNMP management software such as NetSight.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. Values displayed have been accumulated since the last system reboot.

Figure 8-3 RMON Statistics Screen



3583\_44

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.

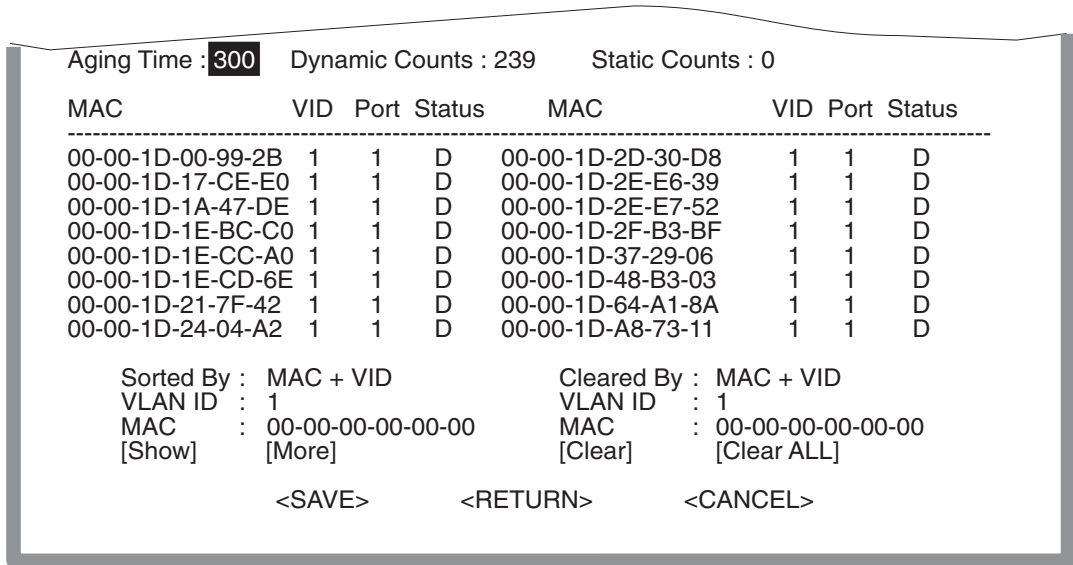
Parameter	Description
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	For 10 Mbps ports, the counter records CRC/alignment errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC/alignment errors and code errors (frame received with rxerror signal).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

Parameter	Description
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Refresh Statistics command	Refreshes the screen.
Reset Counters command	Resets all the counters to zero.

## 8.4 DISPLAYING THE UNICAST ADDRESS TABLE

The Unicast Address Table contains the MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN ID. Using the Unicast Address Table screen ([Figure 8-4](#)), you can search for a specific address, clear the entire address table, or information associated with a specific address, or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.

**Figure 8-4 Unicast Address Table Screen**



3583\_45

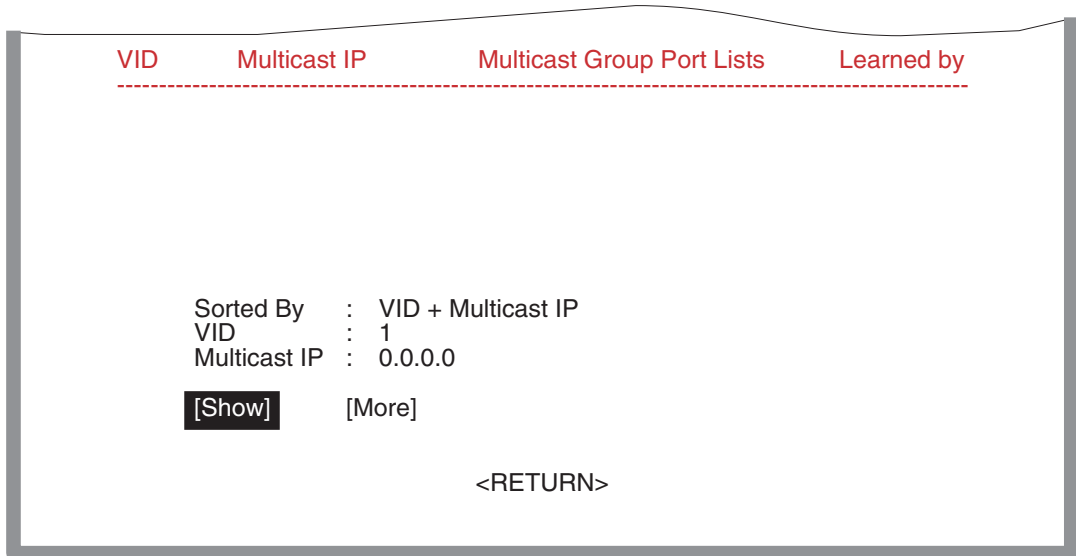
Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 65534 seconds; Default: 300 seconds
Dynamic Counts	The number of dynamically learned addresses in the table.
Static Counts	The number of static addresses in the table.
MAC	The MAC address of a node.
VID	The VLAN(s) associated with this address or port.
Port	The port that includes the MAC address in its address table.
Status	Indicates address status as: D: Dynamically learned, or P: Fixed permanently by SNMP network management software.

Parameter	Description
[Show]	Displays the address table based on specified VLAN ID, and sorted by primary key MAC or VID.
[More]	Scrolls through the entries in the address table.
[Clear]	Clears the specified MAC address.
[Clear All]	Clears all MAC addresses in the table.

## 8.5 DISPLAYING THE IP MULTICAST REGISTRATION TABLE

Use the IP Multicast Registration Table screen (Figure 8-5) to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

Figure 8-5 IP Multicast Registration Table Screen



3583\_46



<b>Parameter</b>	<b>Description</b>
VID	VLAN ID assigned to this multicast group.
Multicast IP	IP address for specific multicast services.
Multicast Group Port Lists	The switch ports registered for the indicated multicast service.
Learned by	Indicates if the ports were learned dynamically or via IGMP.
[Show]	Displays the address table sorted on VID and then Multicast IP.
[More]	Scrolls through the entries in the address table.



# System Restart Menu Screen

This chapter describes the System Restart Menu screen and how to reset the switch or exit a current Local Management session.

## Screen Navigation Path

Password > Main Menu > **System Restart**

## 9.1 RESETTING THE SYSTEM

Select the System Restart Menu item in the Main Menu screen to reset the management agent. The reset screen includes options shown in [Figure 9-1](#) and described in the following table.

**Figure 9-1 System Restart Menu Screen**

Restart Option :

POST	:	<b>YES</b>
Reload Factory Defaults	:	NO
Keep IP Setting	:	NO
Keep User Authentication	:	NO

[Restart]

<SAVE>                      <RETURN>                      <CANCEL>

3583\_47

Parameter	Description
POST	Runs the Power-On Self-Test.
Reload Factory Defaults	Reloads the factory defaults.
Keep IP Setting	Retains the settings defined in the IP Configuration screen described in <a href="#">Section 6.2.1</a> .
Keep User Authentication	Retains the user names and passwords defined in the Console Login Configuration screen described in <a href="#">Section 6.5</a> .

## 9.2 LOGGING OFF THE SYSTEM

To log off the system, use the Exit command in the Main Menu screen to exit the configuration program and terminate communications with the switch for the current session. Refer to [Section 4-1](#) for information about the Main Menu screen.

---

# Configuring and Monitoring the Switch

## 10.1 COMMON TASKS

The switch console menus allow you to modify default switch settings and configure the switch for network management. They also allow you to monitor switch performance and status. Refer to Chapters 1 through 9 for an overview of the menu hierarchy and a description of all menus. The following sections describe common tasks in setting up and operating the switch using the console menus.

To begin, set operating parameters and make sure the network connections are correct by performing these tasks:

- Setting password protection for the switch to prevent unauthorized access to console menus ([Section 10.2](#))
- Assigning an IP address for the switch if you plan to manage the switch using SNMP, or if you use Telnet to access the switch ([Section 10.3](#))
- Checking network configuration status and verifying that network connections are correct ([Section 10.4](#))

After the switch is installed and operating, you may want to perform one or more of the following tasks:

- Connecting via Telnet for in-band access to the console menus ([Section 10.5](#))
- Setting SNMP parameters for management access ([Section 10.6](#))
- Viewing switch statistics to monitor and evaluate switch performance and traffic patterns on the network ([Section 10.7](#))
- Configuring port mirroring ([Section 10.8](#))
- Downloading a software upgrade ([Section 10.9](#))
- Configuring Spanning Tree parameters ([Section 10.10](#))
- Configuring VLANs ([Section 10.11](#))
- Configuring Class of Service ([Section 10.12](#))

- Configuring IGMP multicast filtering ([Section 10.13](#))
- Configuring port operation (enable/disable, port speed, full/half duplex and flow control) ([Section 10.14](#))
- Configuring the Unicast Address table ([Section 10.15](#))
- Setting a default gateway ([Section 10.16](#))
- Configuring SmartTrunks ([Section 10.17](#))

## 10.2 SETTING PASSWORD PROTECTION

The switch is factory-configured with administrator access rights to the console menus set to READ/WRITE. This setting allows anyone to use the console menus to modify any operational parameter. To protect the configuration of the switch from unauthorized modification, you should enable password protection to the console menus.

To enter a password, proceed as follows:

1. Select Management Setup Menu from the Main Menu and press [ENTER].
2. Select Console Login Configuration and press [ENTER].
3. For the “ADMIN” user type, enter a password containing up to 11 alphanumeric characters. Note that the password is not case sensitive.

By factory default, there is no password configured. This means that at the login: prompt, all you have to do is type “admin” for the username and press [Enter] to gain READ/ WRITE access to the console menus. When you configure the password parameter, the factory default setting is deactivated and the new password governs access to the console menus.

If you forget your password, contact your Enterasys Networks Support Representative.



**NOTE:** You are automatically logged out from the console menus based on the Lock-out Time setting in the Console Login Configuration Menu. A setting of “0” permits the console menus to remain available indefinitely.

## 10.3 ASSIGNING AN IP ADDRESS

To assign an IP address to the switch, proceed as follows:

1. Select **Management Setup Menu** from the Main menu.
2. Select **Network Configuration** and then IP Configuration.
3. Highlight the IP address field and enter the IP address. Press ENTER.

The IP address is now set. The subnet mask is automatically set to correspond to the class of the address entered. If a different mask is used on the network, highlight **Subnet Mask** and enter the appropriate mask.

## 10.4 CHECKING NETWORK CONFIGURATION STATUS

To check connection status for the network, proceed as follows:

1. Select **Device Control Menu** from the Main Menu.
2. Select **Port Information** and press ENTER.
3. If a network cable is properly connected to a port, the Link for the port reads UP. If no cable is connected to the port, or if the cable or port is faulty, the Link for the port reads DOWN.
4. If you see a DOWN status for a connected port, plug the cable into another port on the switch or try another cable.

## 10.5 CONNECTING VIA TELNET

You can connect to the switch from a remote location using the Telnet application. This application allows you to establish in-band access to the console menus.

To connect to the switch via Telnet, proceed as follows:

1. Assign an IP address using the Network Configuration Menu.
2. Set a password using the Console Login Configuration Menu.
3. Login to the switch via Telnet using the configured IP address and the password.

## 10.6 SETTING SNMP MANAGEMENT ACCESS

Access to the switch through SNMP is controlled by community names. The community names set for the switch must match those used by the SNMP management station for successful communication to occur. Access for community names can be set to READ/WRITE or READ ONLY access. The default “Public” community name allows READ ONLY access to the device via SNMP, whereas the default “Private” community name allows READ/WRITE access.

The switch can send SNMP messages called traps to SNMP management stations when an important event occurs with the switch. The switch allows up to five destinations to be configured for these trap messages to be sent.

To configure SNMP access for the switch, proceed as follows:

1. Select **Management Setup Menu** from the Main Menu.
2. Select **SNMP Configuration Menu**.
3. Select **SNMP Communities** from the menu. Enter the desired community names (you are permitted to enter from 1 to 20 characters) and set access to **READ/WRITE** or **READ ONLY**.
4. Select **IP Trap Managers** from the SNMP Configuration Menu.
5. Enter appropriate IP addresses for the Trap destinations.
6. For each Trap destination entered, a corresponding access community name should be entered.

## 10.7 VIEWING SWITCH STATISTICS

To view switch statistics, proceed as follows:

1. Select **Network Monitor Menu** from the Main Menu.
2. Select **Port Statistics**. Then select the stack unit, and port to display the main statistical counts for the port.
3. Select **RMON Statistics**. Then select the stack unit, and port to display detailed statistical counts for the port.
4. On any of the statistics screens, select **Reset Counters** to clear (zero) the displayed statistical counts and **Refresh Counters** to refresh (update) the displayed statistical counts.

## 10.8 CONFIGURING PORT MIRRORING

You can mirror the traffic being switched on any port for the purposes of network traffic analysis and connection assurance. When Port Mirroring is enabled, one port becomes a monitor port for any other port within the stack. Note that the source and target ports must be configured within the same VLAN and be operating at the same speed. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

To configure port mirroring, proceed as follows:

1. Select **Device Control Menu** from the Main Menu.
2. Select **Mirror Port Configuration**.



3. For the Mirror Source Port, select the stack unit and port number.
4. For the Mirror Target Port, select the stack unit and port number.
5. Set the Status field to **ENABLED**.
6. Connect a traffic analyzer or RMON probe to the mirroring port.

## 10.9 DOWNLOADING A SOFTWARE UPGRADE

You can upgrade the operational software in the switch without physically opening the switch or being in the same location. The software storage sector in the flash memory of the switch is reprogrammed, allowing you to easily download software feature enhancements and problem fixes to the switch from a local or remote location.

Software can be downloaded to the switch in two ways:

- Via the serial port. This procedure is an out-of-band operation that copies the software through the serial port to the switch. This operation takes approximately three minutes and requires minimal configuration.
- Via TFTP download. This procedure uses a TFTP server connected to the network and downloads the software using the TFTP protocol. A TFTP download is much faster than a serial download, requiring only a few seconds, and can be used to upgrade a switch that is not physically in the area. The disadvantage is that this method requires a TFTP server and additional setup.

### 10.9.1 Downloading via the Serial Port

A serial download is the easiest method to upgrade the switch software, requiring the least amount of equipment and configuration.

To download switch software via the serial port, proceed as follows:

1. With the console port connected, reset the switch by powering the switch off and then on.
2. After the power-on hardware and software tests are complete, the system initialization screen displays the following message:

```
(D)ownload System Image or (S)tart Application: [S]
```

3. Press “D” to download system firmware. The following message displays:

```
Select the Firmware Type to Download (1)Runtime (2)POST  
(3)Mainboard [1]:
```

4. Select “1” to download the agent software. The following messages display:

```
Your Selection: Runtime Code
Download code to FlashROM address 0x02880000
Change Baud Rate to 57600 and Press <ENTER> to Download.
```

5. Change your baud rate to 57600 bps and press ENTER. Send the file using the XMODEM protocol from your computer application (the procedure varies depending upon the application used).

6. When the XMODEM procedure finishes, the following messages are displayed:

```
XModem Download to DRAM buffer area 0x00200000: ... SUCCESS !
Verifying image in DRAM download buffer 0x00200000... SUCCESS !
Update FlashROM Image at 0x02880000 ... SUCCESS !
(D)ownload another Image or (S)tart Application: [S] s
Change Baud Rate to 9600 and Press <ENTER>.
```

7. Press “S” to start the user interface, change your baud rate to back to 9600 bps and press ENTER. The user interface logon screen will then display.

## 10.9.2 Downloading via TFTP

To perform a TFTP download, you must first configure the switch. This consists of programming the switch with an IP address, if this has not already been done, and entering the IP address of the TFTP server and the name of the upgrade file.

To program the switch IP address, select **Management Setup Menu** from the Main Menu screen, then select **Network Configuration**.

To download switch software via TFTP, proceed as follows:

1. Select **Download Server IP Address** from the TFTP Download Menu.
2. Enter the TFTP server IP address and press ENTER.
3. Select **Download Filename** and enter the file name to be downloaded from the TFTP server.



**NOTE:** For a TFTP download, the path to the file must be included in its name. For example, if the upgrade file name is filename.bin and it resides in the directory /usr/tftp on the TFTP server, then you must enter the TFTP file name as: “/usr/tftp/filename.fls”.

4. If necessary, configure the address of an IP gateway to reach the server from the switch using the Gateway IP field in the Network Configuration/IP Configuration menu.

5. Configure the TFTP server by copying the download file from the upgrade disk to an appropriate directory and starting the server.
6. Select **Process TFTP Download** and press ENTER.

To verify that the TFTP download has been successfully completed, note the software version level displayed on the Switch Information screen accessible from the System Information Menu. This number should match the version number that appears on the upgrade disk.

## 10.10 CONFIGURING SPANNING TREE PARAMETERS

The switch supports the IEEE 802.1D Spanning Tree Protocol. This protocol allows redundant connections to be created between LAN segments for purposes of fault tolerance. Two or more physical paths between different segments can be created through the switch, with the Spanning Tree Protocol choosing a single path at any given time and disabling all others.

If the chosen path fails for any reason, a disabled alternative is activated, thereby maintaining the connection. Refer to [Appendix A](#) for further information on using the Spanning Tree Protocol in a network.



**NOTE:** Configuring Spanning Tree parameters from their default can cause serious deterioration of network performance.

To configure Spanning Tree Parameters, do the following:

1. Select the **Device Control Menu** from the Main Menu.
2. Select the **Spanning Tree Configuration Menu** and then **STA Bridge Configuration**.
3. Turn the switch Spanning Tree operation on or off by setting the Spanning Tree Protocol field to ENABLED.
4. From the Spanning Tree Configuration Menu, select **STA Port Configuration**.

The Spanning Tree Port Configuration Menu displays. Change the parameters that display in this menu as required.

## 10.11 CONFIGURING VLANs

A virtual LAN (VLAN) is a group of devices on one or more LANs that are configured such that they can communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

The most fundamental benefit of VLAN technology is the ability to create workgroups based on function rather than on physical location or media. For further information, refer to [Appendix B](#).

To configure VLANs, proceed as follows:

1. Select the **Device Control Menu** from the Main Menu.
2. Select **802.1Q VLAN Static Table Configuration Menu**.
3. In the VID and VLAN Name fields, enter an ID number (1-2048) and a symbolic alphanumeric name (up to 8 characters) to identify the VLAN.
4. Set the Status field to **Active**.
5. Under Egress Ports, select ports by entering “1,” or enter “0” to remove it from the VLAN.
6. Under Forbidden Egress Ports, enter a “1” to prevent a port from being part to this VLAN.
7. To configure other VLANs, select **New** and press ENTER.

## 10.12 CONFIGURING CLASS OF SERVICE

You can configure Class of Service parameters using the 802.1P Port Priority Configuration screen. This screen permits you to configure two priority levels for traffic being forwarded through the switch. During periods of congestion, Class of Service settings ensure that traffic which has been assigned high priority is forwarded through the switch ahead of normal priority traffic. For further information, refer to [Appendix C](#).

To configure Class of Service, proceed as follows:

1. Select **Device Control Menu** from the Main Menu.
2. Select **802.1P Configuration**, then **802.1P Port Priority Configuration**.
3. Set the individual port priorities by entering 0-3 for the low priority queue or 4-7 for the high priority queue.



**NOTE:** Note that the default for all ingress ports is zero.

## 10.13 CONFIGURING IGMP

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For information about the use of IGMP snooping and multicast filtering, refer to [Appendix D](#).)

To configure IGMP operation, proceed as follows:

1. Select **Device Control Menu** from the Main Menu.
2. Select **IGMP Configuration** and press ENTER.
3. Set the IGMP Status to **ENABLED**. This enables the switch to monitor network traffic to determine which hosts want to receive multicast traffic. Default is **DISABLED**.
4. Set the IGMP Query Count to the number of minutes that must elapse before the switch removes the port from an IGMP group. This timer is started after the number of queries are missed as defined in the IGMP Query Count.
5. Set the IGMP Report Delay to the number of queries that must be missed before the IGMP Report Delay timer is started. This is used in conjunction with the IGMP Report Delay to remove ports from an IGMP group.

## 10.14 CONFIGURING PORT OPERATION

You can configure switch ports for operational parameters such as auto-negotiation, duplex mode, port speed and flow control. The 100Base-FX fiber ports always operate in full duplex mode and 100 Mbps speed. Therefore, these two parameters, along with auto-negotiation, are not configurable on these fiber ports.

To configure port operation, proceed as follows:

1. Select **Device Control Menu** from the Main Menu.
2. Select **Port Configuration** and press ENTER.
3. Select the port number to configure.
4. In the Admin column, select **ENABLED**. You can also disable the port due to abnormal behavior or for security reasons.
5. In the Flow Control column, select **ENABLED** to enable flow control, or **DISABLED** to disable it. When enabled, the switch uses back pressure for half duplex and IEEE 802.3x for full duplex. These flow control methods can also be set directly by selecting **BACK\_PRESSURE** or **802.3X**. Note that flow control should not be used if the port is connected to a hub.
6. In the Speed and Duplex column, select **AUTO** to enable Auto-negotiation for the port, or select **1000\_FULL**, **1000\_HALF**, **100\_FULL**, **100\_HALF**, **10\_FULL**, or **10\_HALF**.



**NOTE:** If Auto-negotiation is not enabled, the duplex mode and port speed need to be configured.

## **10.15 CONFIGURING THE UNICAST ADDRESS TABLE**

The Unicast Address Table allows you to designate forwarding treatment through the switch for specific MAC addresses, allowing you to maintain the efficiency and security of your network. In this screen, you can:

- Search for a specific MAC address.
- Clear the entire table or information associated with a specific address.
- Set a port to lock on a specific MAC address to prevent another user from using that port.
- Set the Aging Time for deleting inactive entries.

The switch learns addresses dynamically from incoming packets and builds a table of these addresses along with their associated ports. There are two types of MAC addresses in the forwarding table:

- Dynamic MAC addresses, which are dynamically learned and removed by the switch based on a time period defined using the Aging Time option.
- Static MAC addresses, which are entered manually, stored in nonvolatile memory and automatically placed in the address table.

There are seven types of status that can be configured for each address in the table:

- Permanent, which means that the MAC address is in use and will remain so after the next switch reset.
- Delete On Reset, which means that the MAC address is in use and will remain so until the next switch reset.
- Lock Port, which means set the port to a Lock state according the MAC address. If a MAC address is not entered, then lock the port on the first address the port receives.
- Unlock Port, which means that the locking state is disabled on the selected port.
- Invalid, which will remove the entry.
- Delete On Time Out, which means that the MAC address is in use and will remain so until it is aged out.
- Other, which means that the MAC address is in use but the conditions under which it will remain differ from the preceding values.

To configure the Unicast Address Table, proceed as follows:

1. Select **Network Monitor Menu** from the Main Menu.
2. Select **Unicast Address Table**.
3. As desired, set the Aging Time for the table, or view, search or clear entries by MAC address or VLAN ID.

To configure a specific MAC address in the table, proceed as follows:

1. From the Network Monitor Menu, select **Static Unicast Address Table Configuration**.
2. For the MAC address, specify the VLAN ID, switch port, and the Status (Permanent, Delete On Reset, Lock Port, Unlock Port, Invalid, Delete On Time Out, or Other).
3. Highlight the **Set field** and press ENTER.

### 10.15.1 Port Locking

When a port is locked, the following conditions exist:

- Any existing addresses for the selected port are cleared from the Unicast Table.
- If a MAC address was not entered, then the first address received on the port is locked in and is the only source address recognized on that port.
- If a MAC address was entered, then that MAC address becomes the locked port address.
- Locked Port MAC addresses are displayed with a Status of Lock Port in the Static Unicast Address Table Configuration Menu.
- On the LM Screen under Network Monitor Menu Unicast Address Table, the lock port MAC address entries are displayed with an L.
- Locked Ports are stored in NVRAM and are retained through board resets.
- Re-locking a locked port will clear existing entries and start the lock procedure again, either taking the next MAC address if no MAC entry was entered, or using the entered MAC address.

### 10.15.2 Unlocking the Port

When a port is unlocked, the following conditions exist:

- All locked entries for that port are cleared.
- New MAC Address entries will show up normally.
- Re-unlocking an unlocked port will have no effect.

## 10.16 SETTING A DEFAULT GATEWAY

The default Gateway parameter defines the IP address of a router or other network device to which IP packets are to be sent if destined for a subnet outside of that which the switch is operating.

To set a default gateway, proceed as follows:

1. Select **Management Setup Menu** from the Main Menu.
2. Select **Network Configuration** and then **IP Configuration**.
3. In the field Gateway IP, enter the IP address and press ENTER.

## 10.17 CONFIGURING SMARTTRUNKS

You can configure up to six port trunks on the switch. Each trunk can combine up to eight ports into an aggregate connection with up to 800 Mbps of bandwidth when operating at full duplex. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail.

To configure the port trunks, do the following:

1. Select the **Device Control Menu** from the Main Menu.
2. Select **SmartTrunking Configuration**.
3. Enter a SmartTrunk Group ID number from 1 to 6 to identify the trunk.
4. Select from two to eight ports to configure as one trunk. You can configure up to six trunks per switch unit. The ports used for each trunk must all be on the same internal switch chip, which is synonymous with the SmartTrunk Group ID. [Table 10-1](#) identifies the ports associated with each group ID.

**Table 10-1 SmartTrunk Configuration, Ports Associated with Group IDs**

Group IDs	1	2	3	4	5	6
Ports	1 thru 8	9 thru 16	17 thru 24	25 thru 32	33 thru 40	41 thru 48



**NOTE:** The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.



5. For each Trunk ID, select **ENABLE** to enable the trunk.



**NOTE:** It is advisable to enable the trunk prior to connecting any cable between the switches to avoid creating a loop.

When using port trunks, remember that:

- Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.
- To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.



---

# SNMP Management

## 11.1 THE SNMP PROTOCOL

SNMP (Simple Network Management Protocol) is a communication protocol for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, routers, and host computers. SNMP is typically used to configure these types of devices for proper operation in their network environment, as well as to monitor them to evaluate their performance and detect potential problems.

Managed entities supporting SNMP typically contain software, which runs locally on the device and is referred to as an agent. The software in the switch functions as an agent, monitoring and controlling the functionality of the switch.

A defined set of variables, referred to as managed objects, is maintained by the agent and used to manage the device. These objects are defined in a Management Information Base (MIB) which allows for a standard presentation of the information controlled by the agent over the network.

The software used to access the information maintained by the SNMP agents across a network is referred to as the SNMP Manager, and typically runs on a workstation.

The SNMP manager software uses a MIB specification, equivalent to that which the agent maintains, to read and write objects controlled by the agent for purposes of configuring and monitoring the device. SNMP defines the format of the MIB specifications and the protocol used to access this information.

There are three main operations defined in SNMP:

- GET operations read information from the managed device, such as those used to obtain status or statistical data.
- SET operations change a functional parameter on the device, such as those used to configure Port Speed or to initiate a software download. GET and SET operations are initiated only by the manager software, and result in a response by the agent.
- TRAP operations allow the agent to send an unsolicited message to the manager. This operation is typically used as an alert of a potential problem or a change of status with the device. The Trap Destination parameter in the SNMP Configuration Menu is used to configure the IP addresses of the SNMP Manager to which switch trap messages are sent.

## 11.2 MIB OBJECTS

A number of standard MIB specifications have been defined for managing network equipment. SNMP compliant devices typically support one or more standard MIBs defined by the Internet Engineering Task Force (IETF), in the form of Request for Comments (RFC) documents.

These MIBs provide a common method of managing devices, such as hubs and switches, and network interfaces, such as Ethernet and token ring. The primary standard MIB, referred to as MIB II, provides an overall view of the managed agent and must be supported, at least in part, by all SNMP agents. In addition, proprietary MIB extensions are defined by commercial vendors for managing device-specific functions of their products.

The switch supports six standard MIBs:

- RFC 1213 - Management Information Base for Network Management of TCP/IP based Internets (MIB II)
- RFC 1493 - Definitions of Managed Objects for Bridges
- RFC 1573 - Evolution of the Interfaces Group of MIB II
- RFC 1643 - Definitions of Managed Objects for the Ethernet-like Interface Types (Ethernet-Like MIB)
- RFC 1757 - Remote Network Monitoring Management Information Base
- IEEE 802.1Q - VLAN Bridge Management (Q-MIB)

The switch also supports Enterasys Networks proprietary MIB extensions.

### 11.2.1 RFC 1213 (MIB II)

RFC 1213 provides management of system-level parameters, including TCP/IP protocol-related statistics, IP addressing, and interface statistics for each switch port. MIB II is the standard MIB defined by RFC 1213. All agent devices operating SNMP are required to support at least part of MIB II.

This MIB reports information about the protocols and network interfaces supported on the agent itself, as well as other general information. The MIB is divided into a number of groups, each of which corresponds to a specific protocol or set of information. Some groups are defined in other RFC documents.

The groups specifically defined in RFC 1213 and supported by the switch system software are as follows:

- System – General information about the agent system
- Interfaces – Information about the network interfaces of the system
- Address Translation – Interface address information, both MAC level and network (IP) level
- IP – Statistics and information related to the IP protocol
- ICMP – Statistics and information related to the ICMP protocol
- TCP – Statistics and information related to the TCP protocol
- UDP – Statistics and information related to the UDP protocol
- Transmission – Statistics and information related to the physical network medium to which the system interfaces (e.g., Ethernet, token ring, etc.)
- SNMP – Statistics and information related to the SNMP protocol

### **11.2.2 RFC 1493 (BRIDGE MIB)**

RFC 1493 is a group defined under MIB II. This MIB deals with the operation of the system as an 802.1D-compliant bridge. Areas of functionality supported by this group include Spanning Tree and forwarding table information and configuration.

### **11.2.3 RFC 1573 (INTERFACES EVOLUTION MIB)**

RFC 1573 clarifies and extends the managed objects of the “Interfaces” group of MIB II. This MIB takes account of the evolution in interface types and speeds employed in today’s networks.

### **11.2.4 RFC 1643 (ETHERNET-LIKE MIB)**

RFC 1643 provides management and monitoring for the Ethernet-specific aspects of each port on the switch. This is the Ethernet-specific statistics subgroup of the MIB II Transmission group. This group provides a set of statistics related to Ethernet’s physical level operation. Specifically, error and collision-related statistics are presented.

### **11.2.5 RFC 1757 (RMON MIB)**

RFC 1757 is a group defined under MIB II. This MIB provides management for the RMON aspects of the switch. The switch supports four of the nine groups of RMON defined for Ethernet networks on a per port basis.

### **11.2.6 IEEE 802.1Q (Q MIB)**

This MIB includes the set of managed objects as defined in the IEEE 802.1Q VLAN standard. This MIB provides management for the VLAN aspects of the switch.

### **11.3 ENTERASYS PROPRIETARY MIB EXTENSIONS**

Areas of switch functionality not covered by the standard RFC MIBs are specified in the Enterasys private MIB. This MIB definition is specified separately from MIB II. Areas covered in this MIB include various system, switch, and port level information.

### **11.4 COMPILING MIB EXTENSIONS: ENTERASYS WEBSITE**

The MIBs supported by the switch must be compiled into the SNMP network management platform before the switch can be managed. The supported MIBs are available using the Enterasys website at:

<http://www.enterasys.com>

The four standard MIB specifications listed above with which the switch is compliant are generally available with the SNMP management platform.

---

# Spanning Tree Concepts

## A.1 GENERAL

The IEEE 802.1D Spanning Tree Protocol resolves the problems of physical loops in a network by establishing one primary path between any two switches in a network. Any duplicate paths are barred from use and become standby or blocked paths until the original path fails, at which point they can be brought into service.

### A.1.1 Spanning Tree Features

The switch meets the requirements of the Spanning Tree Protocol (STP) by BEING ABLE TO performing the following functions:

- Create a single spanning tree from any arrangement of switching or bridging elements.



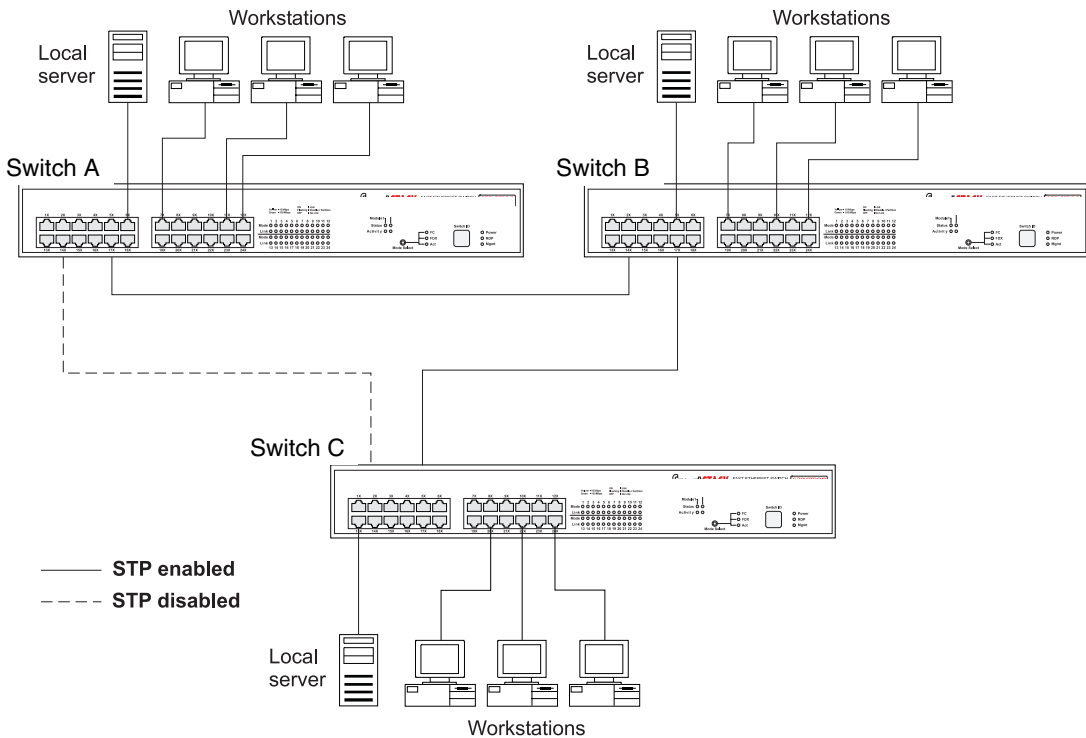
**NOTE:** The term “switch” is used as an equivalent to “bridge” in this document.

- Compensate automatically for the failure, removal, or addition of any device in an active data path.
- Achieve port changes in short time intervals, which establishes a stable active topology quickly with a minimum of network disturbance.
- Use a minimum amount of communications bandwidth to accomplish the operation of the Spanning Tree Protocol.
- Reconfigure the active topology in a manner that is transparent to stations transmitting and receiving data packets.
- Manage the topology in a consistent and reproducible manner through the use of Spanning Tree Protocol parameters.

## A.2 SPANNING TREE PROTOCOL IN A NETWORK

To provide a simple generic example, three standalone switches are shown in [Figure A-1](#) to illustrate how the switches would establish an effective STA configuration. Switches A, B and C are connected together in a redundant topology (more than one path between two points). If the connection between A and B goes down, the link between A and C becomes active, thereby establishing a path between A and B through switch C. Additionally, if the connection between B and C goes down, the link between A and C becomes active, establishing a path between B and C through switch A.

**Figure A-1** Spanning Tree Using Switches





### A.3 SPANNING TREE PROTOCOL PARAMETERS

Several configuration parameters control the operation of the Spanning Tree Protocol. [Table A-1](#) describes the parameters and lists the switch default settings for each parameter.



**NOTE:** You can cause serious network performance degradation if you do not fully understand Spanning Tree concepts. Be sure to consult personnel experienced with this process prior to configuring Spanning Tree parameters.

**Table A-1 Spanning Tree Protocol Defaults**

Parameter	Description	Default Value
Bridge Group Address	Unique MAC group address, recognized by all bridges in the network.	None
Bridge Identifier	Identifier for each bridge. This parameter consists of two parts: a 16-bit bridge priority and a 48-bit network adapter address. Ports are numbered in absolute numbers starting from 1 regardless of their bridge attachment. The network adapter address is the same address as the first port of the bridge.	32768 (bridge priority)
Port Identifier	Identifies each port of each bridge, with an incremental default value given for each port.  Port 1 -32768 Port 9 -32776 Port 17-32784 Port 2 -32769 Port 10 -32777 Port 18 -32785 Port 3 -32770 Port 11 -32778 Port 19 -32786 Port 4 -32771 Port 12 -32779 Port 20 -32787 Port 5 -32772 Port 13 -32780 Port 21 -32788 Port 6 -32773 Port 14 -32781 Port 22 -32789 Port 7 -32774 Port 15 -32782 Port 23 -32790 Port 8 -32775 Port 16 -32783 Port 24 -32791	
Port Priority	Indicates the priority of a specific port in relation to other ports.	128

**Table A-1 Spanning Tree Protocol Defaults (Continued)**

Parameter	Description	Default Value
Cost Component of Each Port	The Spanning Tree Protocol calculates and ensures that an active topology generates minimal cost paths. A value of 100 is generally used for 10 Mbps Ethernet networks, a value of 19 for 100 Mbps Fast Ethernet, and a value of 4 for 1000 Mbps Gigabit Ethernet.	19

For detailed information on the operation of the Spanning Tree Protocol, refer Section 4 of IEEE Standard 802.1D, ISO/IEC 10038:1993.

### **A.3.1 Spanning Tree Protocol Operation**

When the Spanning Tree Protocol is enabled for the first time or when there is a change in the network topology, such as a failure or the addition or removal of a component, the Spanning Tree Protocol automatically sets up the active topology of the current network.

### **A.3.2 Communicating Between Bridges**

Periodically, all devices running the Spanning Tree Protocol on a network transmit packets to each other “in care of” the Bridge Group Address, which all bridges share. When a bridge receives a frame sent to the Bridge Group Address, the bridge’s Spanning Tree Protocol processes the packet. Application software and other LAN segments ignore the packet. Bridges communicate between each other in order to determine the Root Bridge.

### **A.3.3 Selecting a Root Bridge and Designated Bridges**

During communication between bridges, one bridge is determined to have the lowest bridge identifier. This bridge becomes the Root Bridge.

After the Root Bridge has been selected, each LAN segment looks for the bridge that has the lowest cost relative to the Root Bridge. These bridges become Designated Bridges.

### **A.3.4 Selecting Designated Ports**

Each Designated Bridge selects a Designated Port. This port is responsible for forwarding packets to the Root Bridge.

### **A.3.5 Handling Duplicate Paths**

When the active topology of the network is determined, all packets between any two nodes in the network use only one path. Where a duplicate path exists, the non-designated port is put into a blocking state.

### **A.3.6 Remapping Network Topology**

If there is a change in the network topology due to a failure or the removal or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports.

The following describes the five (5) states of the ports when using spanning tree:

- **Blocking:** A port in this state does not participate in the transmission of frames, thus preventing duplication arising through multiple paths existing in the active topology of the bridged LAN.
- **Listening:** A port in this state is preparing to participate in the transmission of frames. The transmission of frames is temporarily disabled in order to prevent temporary loops, which may occur in a bridged LAN during the lifetime of this state as the active topology of the bridged LAN changes.
- **Learning:** A port in this state is preparing to participate in the transmission of frames.
- **Forwarding:** A port in this state is participating in the transmission of frames.
- **Disabled:** A port in this state does not participate in the transmission of frames or the operation of the spanning tree process.



---

## Virtual LANs (VLANs)

### B.1 VLANs AND FRAME TAGGING

The switch supports IEEE 802.1Q-compliant virtual LANs (VLANs). This capability provides a highly efficient architecture for establishing VLANs within a network and for controlling broadcast/multicast traffic between workgroups. Central to this capability is an explicit frame tagging approach for carrying VLAN information between interconnected network devices.

With frame tagging, a four-byte data tag field is appended to frames that cross the network. The tag identifies which VLAN the frame belongs to. The tag may be added to the frame by the end station itself or by a network device, such as a switch. In addition to VLAN information, the relative priority of the frame in the network can be specified by the tag. For more information, refer to ([Appendix D](#)).

VLANs provide greater network efficiency by reducing broadcast traffic, but also allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security, since traffic must pass through a Layer 3 switch or a router to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 1024 VLANs based on the IEEE 802.3Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Two-level priority tagging
- Port trunking with VLANs

### B.2 VLAN CONFIGURATION

VLAN operation on the switch is enabled by default. Therefore, all frames are transferred internally through the switch with a VLAN tag. This tag may already be on the frame entering the switch, or added to the frame by the switch. VLAN information already existing on frames entering the switch is automatically handled by the switch. The switch learns VLAN information from tagged frames and appropriately switches frames out the proper ports based on this information. The configuration of VLANs for frames entering the switch without tags must be made by the user of the switch. This configuration can be made either through the console interface or via SNMP.

#### Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN groups it will participate in. By default, all ports are assigned to VLAN 1 as untagged ports. You should add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and the device at the other end of the link also supports VLANs. Then assign the port at the other end of the link to the same VLANs. However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

Port-based VLANs are tied to specific ports. The switch's forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding and flooding decisions, the switch learns the relationship of the MAC address to its related port—and thus to the VLAN—at run-time.

#### VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways:

- If the frame is untagged, the switch assigns the frame to an associated VLAN based on the PVID of the receiving port.
- If the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

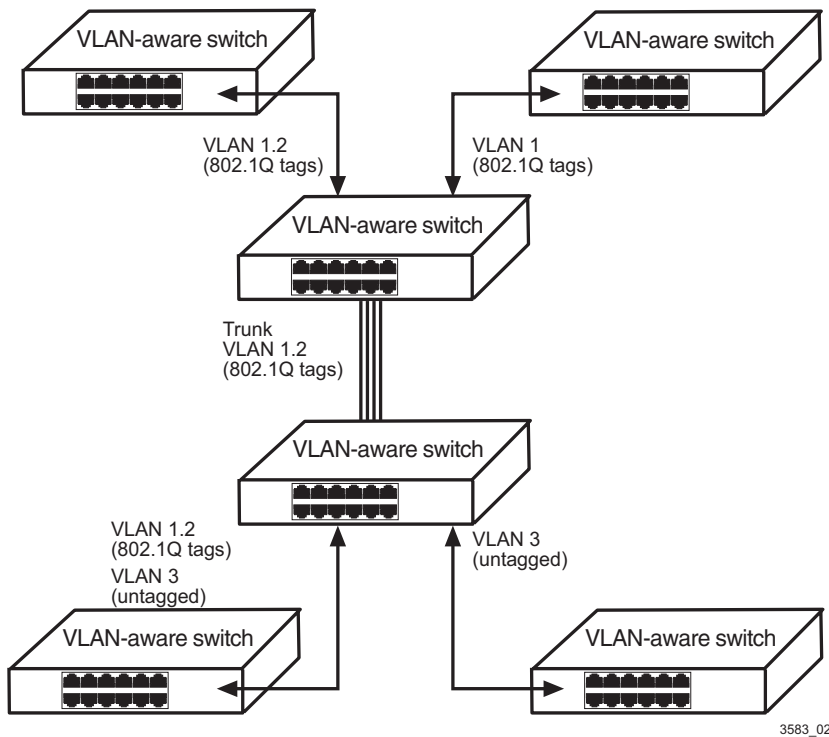
#### Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you must connect them using a router or Layer 3 switch.

## 2.3 FORWARDING TAGGED/UNTAGGED FRAMES

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port's default VID. The default PVID is VLAN 1, but this can be changed as described in [Section 7.15](#).

**Figure B-1 Example of Multi-Switch VLAN Configuration**



## B.4 FORWARDING TRAFFIC WITH UNKNOWN VLAN TAGS

Up to 4096 VLANs are supported by the IEEE 802.1Q standard, but this switch only supports 1024 VLANs. Therefore, if this switch is attached to any device that forwards frames with unknown VLAN tags, or to end stations which issue VLAN registration requests for unknown VLANs, this traffic will be dropped.





---

## Class of Service

Class of Service support on the switch allows you to assign mission-critical data to a higher priority through the switch by delaying less critical traffic during periods of congestion. Higher priority traffic through the switch is serviced first before lower priority traffic. The Class of Service capability of the switch is implemented by a priority queuing mechanism. Class of Service is based on the IEEE 802.1p standard specification and allows you to define two priorities of traffic on each switch port:

- high
- normal

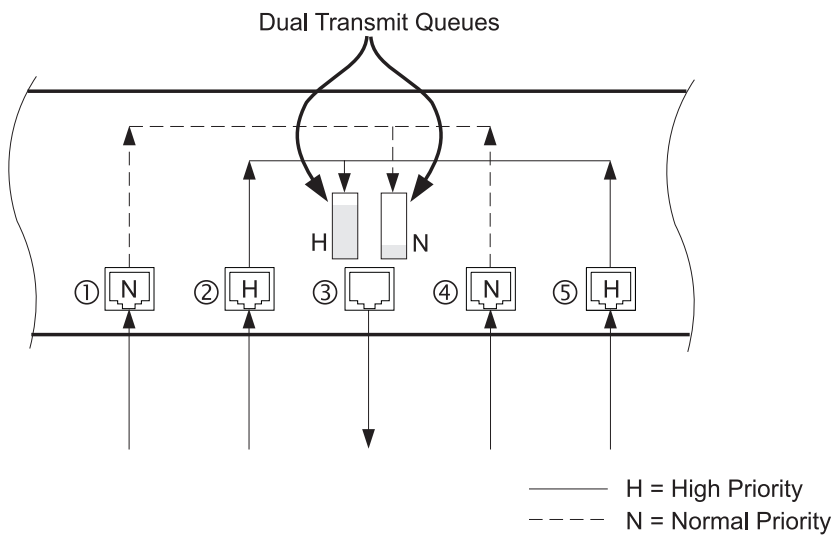
As traffic enters the switch, it is assigned to one of the two priority levels according to information located in the 802.1Q header tag of the frame (refer to [Appendix B](#)) or according to the incoming port number. Frames are then placed into one of two transmit queues on the outbound switch port based on their priority level. Frames on the high priority queue are transmitted first; when that queue empties, traffic on the normal priority queue is transmitted. When priority queuing is being used, each frame that passes through the switch contains a priority level in its header tag. The priority information may already exist in incoming frames, or be assigned by the switch. The determination of individual frame priority is based on the following rules:

1. Incoming tagged frames contain a priority level (range: 0-7).
2. Incoming non-tagged frames are assigned a preconfigured default priority level based on their incoming port (range: 0-7). The assignment of priority per port is done via management using the console interface or via SNMP. See [Section 7.10](#).
3. Priority levels of frames are compared against a preconfigured global priority threshold setting. Those frames with levels equal to or above the threshold are designated high priority traffic; those frames with levels below the threshold are designated normal priority traffic. The default setting for the threshold parameter is: 4 and above = High Priority, 3 and below = Normal Priority.

Properly configured, the Class of Service mechanism assures that during congestion, the highest priority data does not get delayed by normal priority traffic. The tagged header in the frame governs individual frame priority.

Figure C-1 shows priority queuing operating within a switch. Frames entering the switch through ports 1 and 4 are tagged as normal traffic and placed in a normal priority queue on the outbound port. Frames entering through ports 2 and 5 are tagged as high priority traffic and placed in a high priority queue on the outbound port. Priority queuing can be configured using the console interface or via SNMP.

**Figure C-1 Class of Service Example**



---

## IP Multicast Filtering

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast router/switch. The protocol's mechanisms allow a host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer-3, multicast routers use this information, along with a multicast routing protocol, to support IP multicasting across the Internet.

IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with forwarding multicast traffic from the local router/switch to group members on a directly attached subnetwork or LAN segment.

This switch supports IP Multicast Filtering by

- passively snooping on the IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members, and
- actively sending IGMP Query messages to solicit IP Multicast group members.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches instead of flooding to all ports in the subnet (VLAN).

The switch with its IP multicast filtering capability, not only passively monitors IGMP Query and Report messages; it can also actively send IGMP Query messages to learn locations of multicast routers/switches and member hosts in multicast groups within each VLAN.

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, an external IP multicast router is needed if IP multicast packets have to be routed across different subnetworks.



## Numerics

---

5C105 Chassis  
about the [xiii](#)

## A

---

Auto-negotiation, configuration of [10-9](#)

## C

---

Class of Service  
operation of [C-1](#)

Class of Service, configuration of [10-8](#)

community names, SNMP [10-3](#)

Configuring and monitoring the switch

- assigning the IP address [10-3](#)
- checking the network configuration status [10-3](#)
- common tasks involved in [10-1](#)
- configuration of port operation [10-9](#)
- configuration of Unicast Address Table [10-10](#)
- configuring IGMP [10-8](#)
- configuring port mirroring [10-4](#)
- configuring SmartTrunks [10-12](#)
- configuring Spanning Tree parameters [10-7](#)
- configuring the Class of Service [10-8](#)
- configuring VLANs [10-7](#)
- downloading of software upgrades [10-5](#)
- making a Telnet connection [10-3](#)
- setting SNMP management access [10-3](#)
- setting the Gateway IP [10-12](#)
- setting the passwords protection [10-2](#)
- to begin common tasks in [10-1](#)
- viewing the switch statistics [10-4](#)

console lock-out [10-2](#)

Cursor movement [1-3](#)

## D

---

Default switch configuration settings [3-5](#)

Document conventions [xv](#)

Downloads

- serial port for [10-5](#)

downloads

- TFTP [10-5](#)

## F

---

Flow control

- configuration of [10-9](#)

Frame tagging [B-1](#)

## G

---

Gateway IP

- setting of [10-12](#)

Get operations [11-1](#)

Getting help [xvii](#)

## I

---

IGMP [D-1](#)

- configuration of [10-8](#)

IP address

- assigning of [10-3](#)

IP Multicast Filtering

- operation of [D-1](#)

## L

---

Local Management [1-1](#)

- navigating the screens [3-1](#)
- navigating the screens of [1-3](#)
- requirements [1-3, 2-1](#)

---

- requirements for access [1-3](#)
- terminal setup for [2-1](#)
- using Telnet to access [2-4](#)
- Local Management screen hierarchy
  - flow chart of [3-2](#)
- Local Management screens
  - accessing Password screen of [3-1](#)
  - hierarchy of [3-1](#)
  - typical layout of [3-1](#)

## M

---

- MAC address table, configuration of [10-10](#)
- Main Menu screen
  - description of [4-1](#)
- management
  - SNMP access [10-3](#)
- Management agent [1-2](#)
- Management Terminal
  - COM port connection of [2-1](#)
  - setup of [2-2](#)
- manuals
  - web access to [xv](#)
- MIB [11-1](#)
  - compiling extensions [11-4](#)
  - definition [11-1](#)
  - Proprietary [11-4](#)
- MIB objects [11-2](#)
- MIBs, introduction to
  - Compiling MIB Extensions, Enterasys Website [11-4](#)
  - Enterasys Proprietary MIB Extensions [11-4](#)
  - RFC 1213 (MIB-II) [11-2](#)
  - RFC 1757 (RMON MIB) [11-3](#)
- mirror port configuration [10-4](#)
- Moving the cursor [1-3](#)

## N

---

- Navigating screens [3-1](#)
- network configuration status
  - checking the [10-3](#)
- Network management
  - in-band [1-2](#)
  - out-of-band [1-2](#)

## P

---

- password protection
  - setting of [10-2](#)
- Password screen
  - accessing of [3-1](#)
- port configuration
  - priority [10-8](#)
  - trunk ports [10-12](#)
- port mirroring
  - viewing of [10-4](#)
- port operation
  - configuration of [10-9](#)

## R

---

- Related manuals
  - list of [xv](#)
  - web access to [xv](#)

## S

---

- Screens
  - Console Login Configuration [6-14](#)
  - Device Control Menu [7-1](#)
  - Device Control Menu, purpose of [7-1](#)
  - hierarchy of [3-1](#)
  - HTTP Configuration [6-7](#)
  - IP Configuration [6-4](#)

---

IP Connectivity Test [6-6](#)  
IP Trap Managers [6-13](#)  
Main Menu [4-2](#)  
Main Menu, purpose of [4-1](#)  
Management Setup Menu [6-1](#)  
Management Setup Menu, purpose of [6-1](#)  
navigation of [3-1](#)  
Network Configuration [6-3](#)  
Network Monitor Menu, description of [8-1](#)  
Serial Port Configuration [6-8](#)  
SNMP Communities [6-12](#)  
SNMP Configuration Menu [6-10](#)  
Startup Configuration [6-15](#)  
System Information [5-2](#)  
System Information Menu [5-1](#)  
System Information Menu, purpose of [5-1](#)  
System Restart Menu [9-1](#)  
typical layout of [3-1](#)

Serial port  
download [10-5](#)  
downloading software using the [10-5](#)

SET operations [11-1](#)

Setup of  
management terminal [2-2](#)

SmartTrunks  
configuration of [10-12](#)

SNMP  
configuring access [10-3](#)  
management [xiv](#), [11-1](#)  
MIB extensions [11-4](#)  
operations [11-1](#)  
traps [11-1](#)

software upgrades  
downloading of [10-5](#)  
downloading via serial port [10-5](#)  
downloading via TFTP [10-6](#)

Spanning Tree parameters  
configuration of [10-7](#)

Spanning Tree Protocol (IEEE 802.1D)  
concepts of [A-1](#)  
Switch configuration parameters  
default settings of [3-5](#)  
switch statistics  
viewing of [10-4](#)

---

## T

tags, VLAN [B-1](#)  
Telnet  
connecting to switch using [10-3](#)  
Telnet connections [2-4](#)  
TFTP  
download process [10-6](#)  
downloading software [10-5](#)  
traps  
SNMP [11-1](#)

---

## U

Unicast Address Table  
configuration of [10-10](#)

---

## V

VLAN (IEEE 802.1Q)  
forwarding tagged/untagged frames [B-3](#)  
forwarding traffic with unknown VLAN  
tags [B-3](#)  
introduction to [B-1](#)  
VLANs, configuration of [10-7](#)

---

## W

web access to manuals [xv](#)

